BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-115, VOLUME 1

2 JULY 1999

Communications and Information

NETWORK MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCLD (CMSgt Borras) Certified by: HQ USAF/SCXX (Lt Col Pricer)
Supersedes AFI 33-115, 1 June 1998. Pages: 63
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*. It identifies responsibilities for supporting critical Air Force communications and information networks, primarily through network control centers (NCC). Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/XPXP), 203 West Losey Street, Room 1060, Scott AFB IL 62225-5222, through appropriate channels, using Air Force (AF) Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCLD and Headquarters United States Air Force (HQ USAF/SCXX), 1030 Air Force Pentagon, Washington DC 20330-1030. See **Attachment 1** for a listing of references and supporting information. **Attachment 4** identifies the breakdown of network elements, tasks performed, and assigns responsibility.

SUMMARY OF REVISIONS

This change incorporates IC 99-1. It ensures all systems are properly configured with required security patches, correct versions of all software, and a test/validation is performed off-line before restoring to operations. This is a significant step forward in our network operational posture and should lead to improved computer network security. A (|) indicates revision from the previous edition.

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
02 Jul 2000	N/A	-

Title and Subtitle Air Force Instruction 33-115 Volume 1, Communications and Information, Network Management	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the Air Force Pentagon Washington, DC 20330-1250	**Performing Organization Report Number** AFI33-115V1
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes Volume 1 of 2 Volumes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 63	

1. Introduction . This AFI provides the overarching direction and structure for Air Force efforts to operationalize and professionalize the network (O/PTN). The goal of NM is to provide effective, efficient, secure, and reliable information network services used in critical Department of Defense (DoD) and Air Force communications and information processes. The NCC is the single focal point which ensures information flow in-garrison or deployed through professional NM, IPO, and direct customer support for mission operations. This instruction provides the guidance necessary to manage the increasingly complex network environment and provide customers high quality services. Our networks have evolved into mission critical systems supporting Air Expeditionary Forces and joint operations. Continued reliance on information-based weapons systems will drive the need for a cohesive Air Force network. See **Attachment 2** for classes of network elements.

2. Background . The Air Force must organize its limited communications and information resources to match force management and deployment practices, while supporting the combat force structure. Concurrently, the command and control (C2), intelligence, and combat support communities are implementing wide area and local area networks (WAN/LAN) to meet an increasing need for lateral coordination versus the traditional vertical processes. Most of these systems are independently installed and operated, creating fragmented lines of communications. These systems require unique skills to operate and maintain and lead to our current dilemma of sustainment. NCCs provide professional NM capabilities to ensure Air Force networks and systems rapidly respond to and support a full range of peacetime and wartime operational contingencies on a global, regional, and local basis.

3. Hierarchy of Network Management . Air Force NM adheres to the Defense Information Infrastructure Control Concept (DIICC). The DIICC consists of three areas of distributed responsibility at

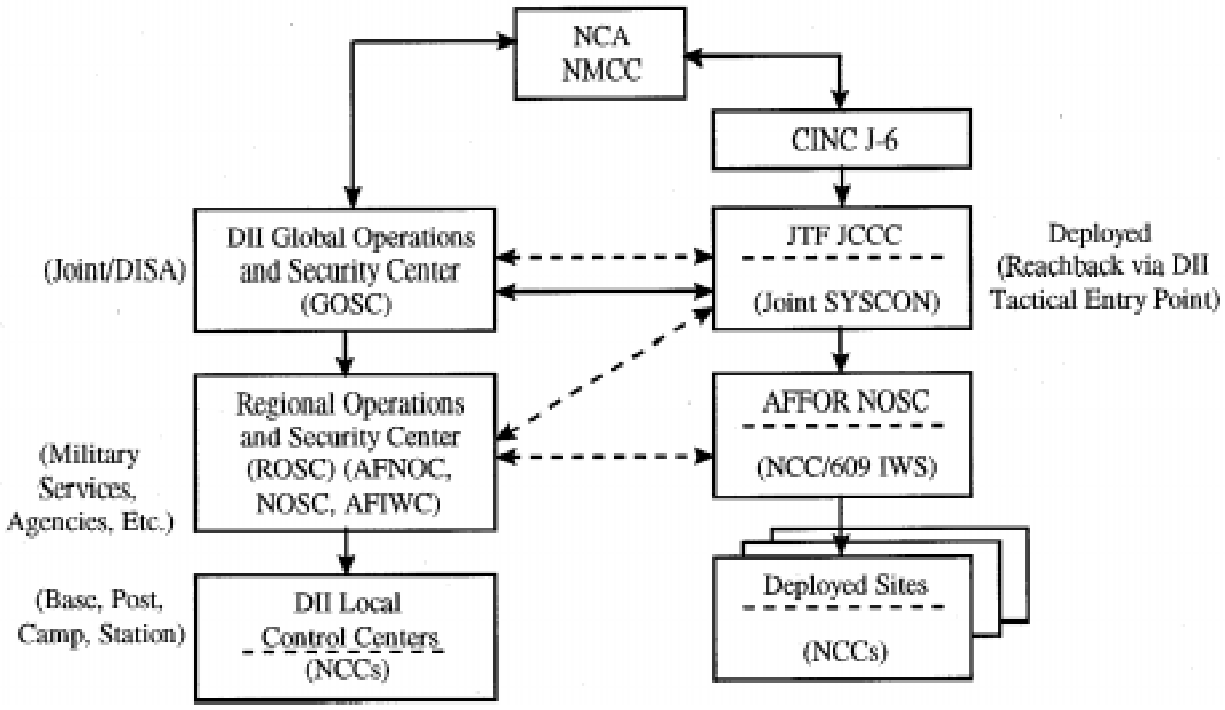
global, regional, and local levels. Air Force NM relationships and responsibilities are matrixed across all three levels.

3.1. The DIICC and NCC Relationship. **Figure 1.** depicts how NCCs fit in the DIICC hierarchical scheme governing NM between the global, regional, and local levels. The associated Joint, Defense Information Systems Agency (DISA), Service, major commands (MAJCOM), and base-level elements are also shown. The lines indicate coordination flow for policy, standards, configuration and NM, and technical coordination of end-to-end information transfer capabilities. These relationships are the means for ensuring global systems interoperate without diminishing the authority of local commanders to direct and manage the information technology and communications assets under their control. Processes and procedures governing these relationships are meant to be complementary and on a non-redundant basis. The correlation between the fixed and equivalent deployed NM hierarchy is also shown in **Figure 1.** The Commander in Chief (CINC)/J-6 establishes the Joint Communications Control Center (JCCC) for the Joint Task Force (JTF) area of responsibility (AOR), and gives direction through the service systems control (SYSCON). The JCCC does the planning and high-level management of the Joint network and provides specific guidance on Joint circuits. DISA's span of control in the deployed environment extends to the JTF SYSCON. The Air Force component SYSCONs and NCCs will use the approved joint suite of NM tools to execute NM responsibilities when deployed. **Table 1.** identifies major responsible support activities aligned with each NM hierarchy.

Table 1. Hierarchy of Network Management.

Network Management	Responsible Support Activity Examples
Global Operations and Security Center (GOSC)	Global Command and Control System (GCCS) Management Center (GMC), Defense Satellite Communications System Operations Center (DSCSOC), SECRET Internet Protocol Router Network (SIPRNET) Management Center, SECRET ATM Management Center
Regional Operations and Security Center (ROSC)	Facility Control Office (FCO), Air Force Network Operations Center (AFNOC), Air Force Information Warfare Center (AFIWC), MAJCOM Network Operations and Security Center (NOSC), Air Force Forces (AFFOR) NOSCs, Community of Interest Air Force Global Weather Central (AFGWC), Medical Systems Implementation and Training Element (MEDSITE)
Local Control Center (LCC)	NCC, System Administrator (SA), WM Community of Interest--Medical Treatment Facility, tenant system

Figure 1. External Network Management Hierarchy and Relationships.



3.1.1. Global, Regional, and Local Services.

3.1.1.1. Global. DISA's GOSC is responsible for the worldwide management and operational oversight of the Defense Information Infrastructure (DII). Enterprise network and systems management policy and standards are developed jointly by DISA, the services, and agencies. The AFNOC and NCCs apply and enforce these policies at the regional and local levels. DISA NM's span of control ends at the base service delivery points (SDP) for fixed communications, and at the Joint SYSCON for deployed. DISA will have visibility into the base network, as required, through a read-only capability and the base will have a similar capability into the Defense Information System Network (DISN) and information processing activities. All DoD organizations have a responsibility to share network trouble report information and analysis data. Electronic exchange of this information allows operations and maintenance management and higher level NM functions to retrieve or query raw data to compile analysis reports.

3.1.1.2. Regional. ROSCs such as the AFNOC, MAJCOM NOSCs, and DISA ROSCs execute network and system management to ensure operational control and information assurance of a specific geographic or global AOR. DISA ROSCs exist in the continental United States (CONUS), Pacific, and European theaters. The AFFOR NOSC is responsible for deployed Air Force NM and reports to the JTF JCCC. Communities of interest also have NM capabilities at this level (e.g., Air Force Personnel Center, AFGWC, MEDSITE, etc.).

3.1.1.2.1. Communities of Interest. A global or regional control center may support and control these communities in the resolution of system problems. The global or regional unit may install an NCC compliant network management system (NMS) at each local unit it controls to enable the local unit to resolve its own network problems within its customer response requirements. This will also decentralize collection of local network performance data for planning purposes. Configure each local NMS to provide status and performance information to the global or regional servers over the WAN. ROSCs ensure LCCs in their AOR collect and forward network and system management data to the GOSC or the appropriate ROSC in a timely manner. However, local units must operate their networks and their NMS in coordination with their base NCC. The following steps are required:

3.1.1.2.1.1. You must negotiate a service level agreement (SLA) between each local unit, your NCC, and the global or regional NM element. If a SLA is already in place, you must review it to ensure NM operations are properly addressed (see paragraph **4.**).

3.1.1.2.1.2. The NCC will assume NM support responsibilities when the NCC has achieved the manpower and equipment necessary to meet the customer response requirements defined by the local unit. Those NCCs taking on this responsibility must configure their systems to provide the global or regional NM element with the required local network status and performance data.

3.1.1.2.1.3. Ensure you minimize duplication of effort. The SLA should contain clear demarcation points for network device management between the local NMS and the NCC, and you should make every effort to reduce overlap of network discovery and mapping of the local area.

3.1.1.2.1.4. The SLA must describe procedures for allowing NM traffic through the NCC's base network security system. Detailed network security issues are outlined in

paragraph **3.1.1.2.3.**.

3.1.1.2.1.5. The SLA must contain escalation procedures that state the flow of trouble calls from local units to the NCC and/or to the global or regional NM element. The AFNOC centrally manages the unclassified and classified data networks and serves as the central design activity for all NCCs. The AFIWC oversees and maintains current status of the security posture of Air Force networks and systems. NCCs provide support to base customers for regional and community of interest services.

3.1.1.2.2. WAN Utilization. NM via the Simple Network Management Protocol Version 1 (SNMPv1) is bandwidth-intensive. To alleviate some of the bandwidth requirements for SNMPv1, move its polling as close as possible to the managed devices. The global or regional NM element must keep its requirements for server-to-server data updates to a minimum, and will move as much batch updating as possible to off-peak traffic periods.

3.1.1.2.3. Network Security. Global or regional NM element operations require SNMPv1 access through base networks to local unit equipment. However, NM via SNMPv1 is inherently unsecure, and you must tightly control it. You must reflect this access in the base network security policy, and the designated approval authority (DAA) must consider this risk created by the global or regional requirement in their accreditation decision. The DAA may choose to accept this risk or require additional countermeasures.

3.1.1.2.3.1. NCCs institute packet filtering on base gateway routers or firewalls to eliminate undesirable incoming SNMPv1 traffic. However, they may have to accommodate SNMPv1 traffic between the global or regional NM element, the local unit NMS, and local unit network devices. The global or regional NM element provides the range of IP subnet addresses for their NM equipment, and the local unit provides the range of local unit IP subnet addresses that the global or regional NM element must access. Keep the width of these ranges to a minimum. If an NCC takes on the NM requirements of a local unit, you must provide SNMPv1 access between the global or regional NM element and the NCC NMS.

3.1.1.2.3.2. The global or regional NM element should investigate the possibility of using encrypted tunnels between the global or regional NM element and local units to reduce the risks of remote management. When approved, the global or regional NM element provides guidance on accommodating this encrypted data stream through base network security systems. This must be done according to Air Force Systems Security Instruction (AFSSI) 4100, (C) *Communications Security Program (U)*.

3.1.1.2.3.3. The local unit must ensure the NMS conforms to all appropriate system guidelines (i.e., system security, software licensing, inventory control).

3.1.1.2.3.4. When the community of interest has a legitimate requirement for a NM capability within their global, regional, or local units, a NMS platform is permitted. However, close coordination is required between the communications and information systems officer (CSO) and the community of interest at all levels to ensure this capability is exercised prudently, securely, and with no duplication of effort.

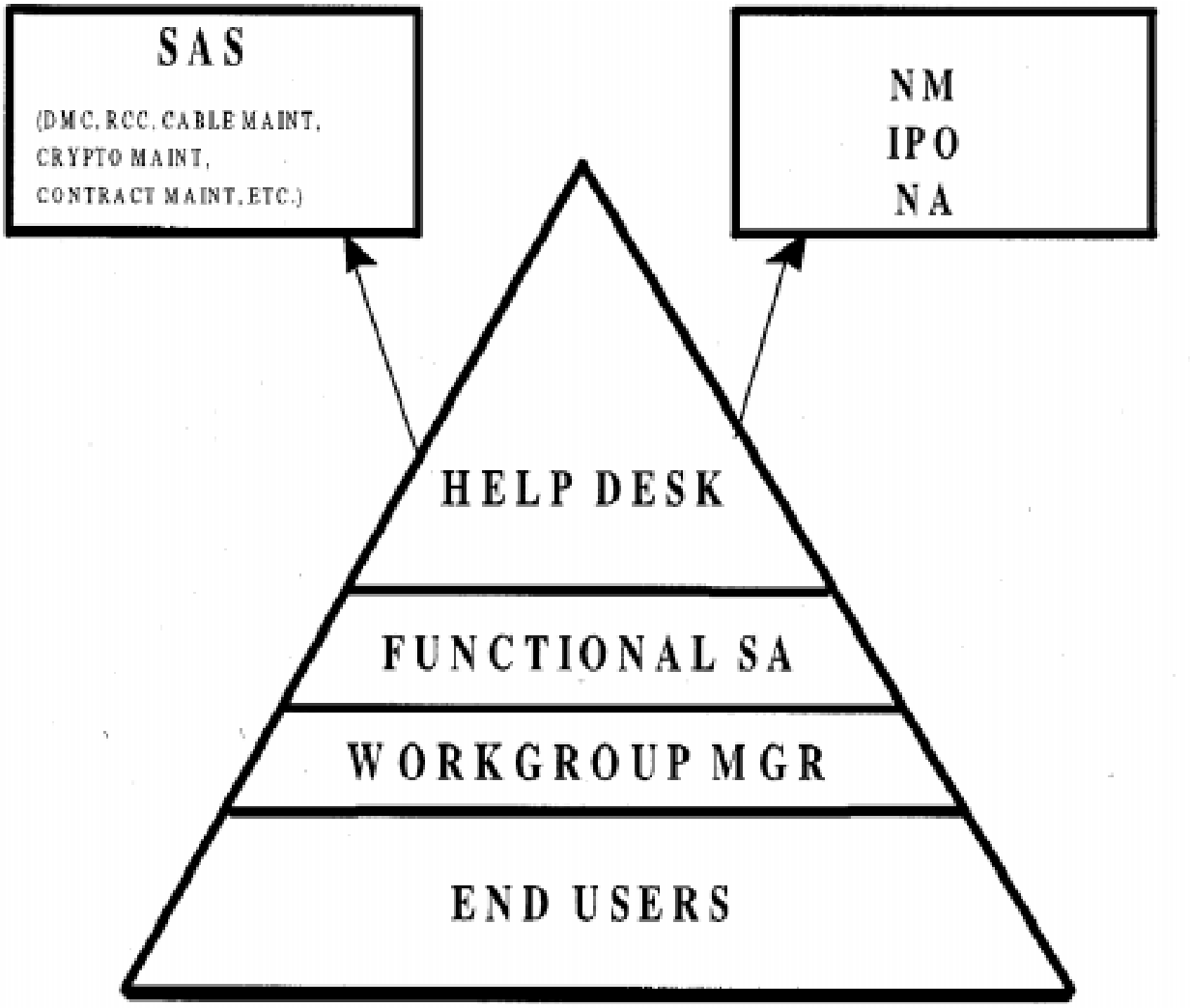
3.1.1.3. Local. LCCs, specifically called NCCs in the Air Force, perform network and system element management. NCCs take direction from the GOSC or the ROSC in accordance with established directives and instructions. An NCC may provide service at the regional or global

level under special circumstances. Community of interest functions may reside at this level, but usually support only a selected set of centralized information processing customers in a functional community. Community of interest LCCs take direction from the NCC.

3.1.2. NCC Organizational Structure and Relationships.

3.1.2.1. NCC. The NCC provides responsive mission support by managing the local infrastructure that provides customers the communications and information resources needed to achieve their operational objectives. The NCC serves as the single focal point for base NM and problem resolution, and is the single logical SDP for all communications traversing the base network. Communications and information services entering and exiting the base or site fall under the operational control of the NCC. Organizations choosing to use other than NCC-provided SDPs, although tied to the base physical infrastructure, are denied direct logical access to the base network to maintain the integrity and security of the base's local infrastructure. The NCC uses collocated independent NM systems, remote support tool sets, and consolidated personnel to respond rapidly to a full range of peacetime and wartime contingencies. The NCC must utilize and adhere to applicable publications to include the DISA publications and circulars, the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6231.07A, *Manual for Employing Joint Communications Systems - Joint Network Management and Control*, January 1995, and all other appropriate Joint and Air Force guidance and instructions. The NCC manages network and systems maintenance for all base users. The NCC performs network and system administration to include security, fault, configuration, performance, and accounting management in their AOR. It oversees network and system operations and manages the exchange of information through the base SDP. This includes network and systems administration operations conducted by other LCC-level network operations centers (e.g., tenant unit LCCs). The NCC cooperative team includes: network operators who perform HD and IPOs, NM, and network administration (NA) within the NCC, and functional systems administration, workgroup management, and specific area support external to the NCC. The NCC trains FSAs and WMs to perform their duties. **Figure 2.** depicts this team's problem resolution approach.

Figure 2. Network Control Center Services Problem Resolution.



3.1.2.1.1. HD Operations. The HD is the base's focal point for problem resolution and is the user's primary point of contact (POC) for problems which WMs or FSAs cannot resolve. The HD provides a central repository for technical advice and solutions for network systems, software applications assistance, automatic data processing support, hardware exchange, and repair service support. It also routes problems it cannot handle to other NCC functional areas, to the Defense megacenters (DMC) or, if necessary, to other technical support agencies such as DISA, AFNOC, and MAJCOM NOSCs. The HD determines the type of reported system problem, reports the status of problem resolution to the affected customer, and maintains a historical data base of problem resolution.

3.1.2.1.2. NM. Provides proactive and reactive management of resources by monitoring and controlling the network, available bandwidth, hardware, and distributed software resources. NM responds to detected security incidents, network faults (errors) and user reported outages at the time of HD referral. If NM personnel cannot resolve a customer complaint or query, the HD refers the problem to a system specialist in the specific area

support function.

3.1.2.1.3. IPO. Conduct IPO according to AFPD 33-2, *Information Protection*, the AFI 33-200 series, and the specialized security publications prescribed in AFI 33-206, *Air Force Specialized Information Protection Publications*. IPO is a critical sub-component of the NM function that implements and enforces national, DoD, and Air Force security policies and directives. It provides proactive security functions established to assist Air Force organizations in deterring, detecting, isolating, containing, and recovering from information system (IS) and network security intrusions. The NCC conducts IPO employing hardware and software tools to enhance the security of their networks. It installs, monitors, and directs proactive and reactive network information protection defensive measures to ensure the availability, integrity, and reliability of base networked and stand-alone information resources. It will coordinate implementation of these solutions with the HD, NM, and customer representatives.

3.1.2.1.4. NA. The network operator assigned to perform NA is assigned directly to the NCC and centrally manages various functional area LANs from the network hardware software operating systems level. Tasks include all core services provided by the NCC to the base populace. These network operators are the base experts in system administration and also provide technical assistance to FSAs and WMs who provide administration support from their servers to their end-user workstations.

3.1.2.1.5. FSA. A FSA is not assigned to the NCC; however, they still take direction from the NCC. They must thoroughly understand the customer's mission, and stay completely knowledgeable of the hardware and software capabilities and limitations. The FSA's area of responsibility is from the user's terminal to the server, but does not include the network backbone infrastructure components. FSAs ensure servers, workstations, peripherals, communication devices, and software are on-line and available to support customers. FSA responsibilities for functional area LANs can be transferred to the NCC if a memorandum of understanding (MOU), memorandum of agreement (MOA), or SLA outlining the terms and conditions is signed between the NCC provider and the recipient. NCC NAs do not operate the end-users' application software, perform data entry, perform database administration, or otherwise manipulate customer data. FSAs contact the HD as necessary if they cannot resolve a problem.

3.1.2.1.6. Workgroup Management. The WM is normally a duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help customers contact to resolve problems. The WM should be an Air Force specialty code (AFSC) 3A0X1 (Information Manager). Information managers receive 3/7 level training on workgroup administration, a significant part of WM duties. When a 3A0X1 is not assigned, any AFSC or occupational series can perform WM duties once trained and certified. WMs are usually not assigned to the NCC, though are logically an extension of the HD team. WMs take direction from the FSA and NCC. NCC direction takes precedence over FSA direction. WMs possess developed knowledge of hardware, software, and communications principles, and install, configure, and operate client/server devices. They resolve the day-to-day administrative and technical system problems users experience and contact their FSA or HD if they cannot resolve their problem.

3.1.2.1.7. Specific Area Support. Specific area support is the set of specialists for

resolving those classes of problems associated with the various elements of the base infrastructure that HD personnel are not trained or equipped to address. Specific area support determines if the HD has correctly classified and assigned the problem, dispatches on-site maintenance, and reports results back to the HD. Specific area support is not normally assigned to the NCC; however, they are functionally accessible resources both in peacetime and wartime, in-garrison and deployed.

4. Standard Level of Service, Service Level Agreements, and Guidance Dis tribution.

4.1. The NCC assists the wing or its functional equivalent in developing a standard level of service, that defines the roles of both the NCC and its customers, to include tenant units. This includes, but is not limited to, network service availability rates, fault response times, NCC dispatch responsibilities, configuration change procedures, initial contingency support requirements, fee-for-service charges (where applicable), customer escalation and security management procedures, and other NCC-provided services. It also defines the customer's role and responsibilities, to include but is not limited to, reporting and escalation procedures, as well as guidance on configuration and systems management.

4.1.1. The NCC coordinates SLAs with customers whose network support requirements are unique or exceed the standard of service. SLAs define division of responsibilities for network operations and services between NCC and customer functional areas. They also define resources both parties will provide to support delivery of negotiated services. CSOs negotiate all SLAs with tenant and outside organizations (see **Attachment 3**).

4.1.2. When necessary, they formalize agreements through MOUs or MOAs, or supplements to this instruction.

4.2. CSOs distribute procedural changes via message traffic or electronic bulletin board. They use electronic bulletin boards, if possible, to distribute handbooks created by the NCC. The wing or its functional equivalent ensures the standard level of service is reviewed at least annually for accuracy.

5. Classified Network Management . Perform classified NM separately from unclassified NM. Ideally, perform classified NM on an infrastructure physically separate from the unclassified network infrastructure. The following concerns come into play when both a classified and unclassified network share a common backbone.

5.1. Denial of service attacks on the unclassified network can disrupt C2 functions on the classified network.

5.2. Using encryption over an unclassified network is an operations security (OPSEC) concern. It provides an easy target for intelligence gathering since the enemy can easily recognize the use of encrypted packets as indicators of possible operations.

5.3. Detecting a network attack is not an easy task. Disconnecting the classified side from the unclassified side (where the attack is coming from) is only viable after the base recognizes an attack is occurring.

6. Responsibilities .

6.1. HQ AFCA:

6.1.1. Establishes and maintains an electronic repository that includes:

6.1.1.1. Communications and information management standards.

6.1.1.2. Current policy and procedures.

6.1.1.3. Lessons learned.

6.1.1.4. Training sources.

6.1.1.5. Training modules.

6.2. MAJCOMs:

6.2.1. Equip each NM site with the resources it needs to meet:

6.2.1.1. Service response times.

6.2.1.2. Service availability standards.

6.2.1.3. Service degradation or failure restoration times.

6.2.1.4. User or subscriber education and training needs.

6.2.1.5. Deployment or contingency support requirements.

6.2.1.6. Network security monitoring and protection.

6.2.1.7. Vulnerability assessment.

6.2.1.8. Security incident reporting and response.

6.2.1.9. Network mapping.

6.2.2. Provide requested unit procedures, checklists, handouts, and training materials to HQ AFCA/GCLD for distribution to other USAF and DoD organizations.

6.3. Bases:

6.3.1. Identify requirements to support NM functions tasked to wings, bases, or units.

6.3.1.1. Work with the systems telecommunications engineering manager - base level (STEM-B) and - command level (STEM-C) to define and integrate technical solutions to the base blueprint for funding prioritization and future implementation.

6.3.2. Use Air Force 33-series publications and negotiated support agreements as a reference to imbed centralized NM support requirements and concepts in performance work statement definitions during initial, renegotiated, or amended contracting actions.

6.3.3. Allocate to each NM area enough resources to meet service provisioning response times, service availability standards, service degradation or failure restoral times, user or subscriber education and training needs, network security monitoring and protection, vulnerability assessment, security incident reporting and response, network mapping, and deployment or contingency support requirements. Workload transferred from other activities must be accompanied by adequate resources (i.e., tenant or functional systems moved into the NCC.)

6.3.4. Establish or consolidate required NM areas subordinate to the NCC according to user or subscriber negotiated SLAs, system or network performance specifications, and minimum local NM quality of service standards.

6.3.5. Establish briefing and reporting requirements (frequency and format) for infrastructure status, performance, and quality of service to aid base-level decision-making regarding infrastructure changes, procedures, training, and other issues.

6.3.6. Support host and tenant organization missions.

6.3.7. Evaluate the level of services provided by each NM location according to system or network performance standards. Direct changes in procedures, allocation of resources, or training methods to minimize resource requirements and improve quality of service.

6.3.8. Establish a wing-level (or equivalent) steering group to develop base policy and procedures for migrating NM toward the Air Force and joint architectures and standards. Target stand-alone and redundant NM capabilities and responsibilities for consolidation to minimize the amount of resources used to do NM while optimizing performance and quality of service.

6.3.9. Report the recommendations to the wing-level (or equivalent) steering group and the STEM-B for inclusion in the base blueprint.

6.4. NCC:

6.4.1. Provides and/or performs the following network services according to established policy, SLAs, MOAs, and MOUs:

6.4.1.1. Allocation and minor engineering.

6.4.1.2. Installation.

6.4.1.3. Quality control (QC) and QA.

6.4.1.4. NM operations and security.

6.4.1.5. Education and training.

6.4.1.6. Remotely provides equivalent service for unmanned sites or facilities, when required.

6.4.1.7. Establishes a HD function as the base's single focal point for communications and information problems.

6.4.1.8. Serves as local support for customers and systems of the Defense Message System (DMS), DISN, regional processing centers (RPC), and community of interest areas in accordance with DISA circulars (DISAC), negotiated support agreements, and the Air Force 33-series publications.

6.4.1.9. Performs as contractor QA evaluator for NCC-monitored communication service contracts.

6.4.1.10. Supports small and minicomputer hardware and software for the small computer systems element as stated in AFI 33-112 and AFI 33-114, *Software Management*.

6.4.1.11. Provides sustainment support for base standard base-level computer customers.

6.4.1.12. Acts as DISN node site coordinator as defined in DISAC P70-series and Air Force 33-series publications.

6.4.1.13. Provides deployed systems and NM services as tasked by the wing commander or equivalent.

6.4.1.14. Defines critical network outages that impact mission capability and up-channel report to the wing commander or equivalent.

6.4.1.15. Uses Air Force 33-series publications and applicable DoD, Joint, DISA, and USAF publications to govern and guide network operations.

6.4.1.16. Participates in the Quality Air Force process, requirements technical solution evaluation process, interfunctional support negotiations, procedural definition process, and workgroups.

6.4.1.17. Identifies and defends, through the base CSO, resource and training requirements to optimize domain service delivery and capability, including support for deployment and contingency operations. Reallocates resources to higher levels, when possible.

6.4.1.18. Establishes performance and quality of service standards for each class of connection and service. Uses DoD and USAF standards, unless more stringent standards are negotiated.

6.4.1.19. Sponsors education and training seminars for users, subscribers, and infrastructure technicians. Supplements material given in other training programs. Orients education toward improving the infrastructure quality of service and security.

6.4.1.20. Trains personnel to:

6.4.1.20.1. Allocate and configure services and resources.

6.4.1.20.2. Control quality of NM operations.

6.4.1.20.3. Administer security.

6.4.1.20.4. Administer data bases.

6.4.1.20.5. Certify training and positions.

6.4.1.20.6. Install systems.

6.4.1.20.7. Manage and respond to trouble calls.

6.4.1.20.8. Perform NM system operations (e.g., configuration, fault, performance, security, and accounting management).

6.4.1.20.9. Educate and train customers.

6.4.1.20.10. Perform line replaceable unit (LRU) level maintenance on network hardware (e.g., servers, personal computers [PC], routers, hubs, and switches).

6.4.1.21. Establishes a position certification program for each position within the organization. Position certification enhances user and subscriber services by making sure assigned personnel are adequately trained.

6.4.1.22. Gathers and analyzes performance data on services provided by the infrastructure domain or domains within the NM area's span of control. Recommends corrections for service problems (e.g., configuration or procedure changes, additional training, equipment upgrades, and additional test devices).

6.4.1.23. Sends MAJCOMs a copy of internally developed or modified procedures, agreements, process flowlists, checklists, informational handouts, and training materials for review,

consolidation, and reissue by other USAF and DoD organizations.

6.4.1.24. Develops, coordinates, and maintains support plans for contingency, service restoration, unit type code requirements, and deployed capability. Validates and tests plans regularly.

6.4.1.25. Manages resources within a NM area's domain through automated processes for such things as permissions, scheduling, database administration, memory backups, and memory and file allocation.

6.4.1.26. Implements, operates, and maintains appropriate security measures.

6.4.1.27. Maintains, or has access to, a library of DoD, Joint, USAF, and MAJCOM publications, commercial manuals, training material, and technical orders for operations and maintenance of domain resources.

6.4.1.28. Keeps an inventory of base and long-haul telecommunications equipment.

6.4.1.29. Develops and maintains a network configuration map and/or developed data base that documents the network infrastructure to include the number of servers and terminals supported.

6.4.2. NA. Provides core network services which include a suite of common services to base customers. They are responsible for configuring, installing, and managing the following data services as required, as well as any other additional services required by local policy and procedures. Most fixed NCCs provide these services. Deployed NCCs provide these services locally or from another site, depending on the NMS suite and mission size.

6.4.2.1. Internet Protocol (IP) Address Management. Acquire control of all base IP address space and manage it through utilization of Dynamic Host Configuration Protocol (DHCP), Bootp, or static configuration. Once control is established, the NCC introduces the Network Address Translator (NAT) to support the base information protection (BIP) boundary.

6.4.2.2. Domain Name System (DNS). Implement a DNS server to resolve host names into IP addresses. DNS is a hierarchical, distributed method of organizing the name space of the Internet. The DNS administratively groups hosts into a hierarchy of authority that allows you to widely distribute and maintain addressing and other information. DNS eliminates the dependence on a centrally maintained file that maps host names to addresses.

6.4.2.3. Messaging Services. Core messaging services offered include, but are not limited to, DMS, Automated Digital Network (AUTODIN), and electronic mail (e-mail) services.

6.4.2.3.1. DMS, designed to replace AUTODIN and e-mail services, is a program established by the DoD to replace and standardize all of its messaging systems, both organizational and individual, over a 20-year period. The DMS provides global connectivity, interoperability, multi-media attachments to messages, and end-to-end security. DMS addresses the operational need for providing secure, accountable, reliable writer-to-reader messaging for the warfighter at reduced cost.

6.4.2.3.2. The Air Force will continue to offer current simple mail transfer protocol (SMTP) and AUTODIN services until all end-users migrate to a fully implemented and operational DMS.

6.4.2.4. Remote Dial-In Communications. The NCCs provide a communications server capable of handling dial-in and dial-out services. Place this server outside the BIP boundary to prevent the possibility of back-door access. This means that internal organizations will not connect external access devices to their local network unless the NCC logically isolates them from the base network. The NCCs control all remote dial-in/dial-out communications services.

6.4.2.5. Office Automation Application Support Services. NCCs/wings develop a core set of supported applications. HD personnel must know the applications the wing supports. Each NCC provides software assistance support for the wing's core set of applications.

6.4.2.6. Non-Classified IP Router Network (NIPRNET)/SIPRNET/Internet Access Service. Mission critical systems and functional operations are rapidly migrating to Transmission Control Protocol/Internet Protocol (TCP/IP) applications. The NCCs control and provide all access to NIPRNET/SIPRNET and the Internet.

6.4.2.7. Network Directory Services (NDS). The NCCs provide a global naming service that maintains information on, and provides access to, every resource on the network, including users, groups, printers, volumes, and servers. NDSs manage all network resources as objects in the network directory data base, independent of their actual physical location. NDS are global to the network, and information is replicated so that local failure cannot bring down the entire system (examples include Novell NetWare 4.x NDS, Windows NT File System, etc.).

6.4.2.8. Remote Distributed Print Services. The NCC provides support to local customers using the DMC services. They provide print management (i.e., print and distribute listing for IS users without distributive print workstations) to include print services within the NCC, remote distributed print services, and organizational network server printers for which the NCC has an SLA.

6.4.2.9. Network Time Protocol (NTP). The NCCs will not allow external NTP sources through the BIP boundary due to inherent security problems. They will utilize NTP within the BIP boundary to synchronize system clocks with a local Global Positioning System (GPS) receiver.

6.4.2.10. New Technologies. The NCC establishes methods to manage new network technologies as they develop to evaluate impact to the base network.

6.4.2.11. Implements software patches and security fixes as required by the NCC, NOSC, AFCERT, AFNOC, or program manager. Tests and validates the proper operation and configuration with appropriate patches and fixes, as required above, prior to restoring any device to the network.

6.4.3. NCC NM:

6.4.3.1. Configuration Management.

6.4.3.1.1. Controls all service points to the base network. The NCC makes sure all service points have functional layout diagrams, hardware interconnection listings, test point location listings, and expected signal characteristics at each test point. It also sees that the service points have hardware labels that clearly identify individual circuit connections and test points. If the service point is too small to contain the above information, the NCC maintains copies for dispatch technicians to use. You must note in the service point

information any changes in the service point configuration or in service operation.

6.4.3.1.2. Works with STEMs and participates in the review and planning of base transmission media and telecommunications systems networks. Makes sure replacements for legacy or dumb network devices incorporate remote support capability to improve centralized NM performance and quality.

6.4.3.1.3. Remotely performs the functions and duties of a Defense Communications System (DCS) Primary Systems Control Facility (PSCF), patch and test facility, DCS switching center, or other DCS operations function, when it is technically and economically feasible and does not degrade quality of service in accordance with DISA procedures. To support the wing during contingencies, the NCC takes over the responsibility and authority of the PSCF for DCS service control.

6.4.3.1.4. Remotely configures user and subscriber terminals, computer hardware and software resources, intrabase and long-haul (tail) circuits, systems, and networks. Base any reconfiguration on subscriber service requirements, network traffic patterns and loading, and results of QA tests.

6.4.3.1.5. The network manager's AOR extends from the interface of the user's terminal to the interfaces of the base-level host, base-level server, or transmission system providing connectivity to off-base assets and includes all the base network backbone infrastructure components.

6.4.3.1.6. Reconfigures equipment or mode of operation by replacing, restrapping, or reprogramming circuit boards, modules, subassemblies, and assemblies.

6.4.3.1.7. Maintains, manages, controls, and distributes the IP address space allocated to the base internet.

6.4.3.1.8. Establishes, maintains, controls, and enforces the base internet use policy (see AFI 33-129, *Transmission of Information Via the Internet*).

6.4.3.1.9. Provides a communications server capable of handling dial-in and dial-out services (see paragraph **6.4.2.4.**).

6.4.3.1.10. Provides monthly initial operational capability/final operational capability (FOC) status metrics to the DAA for tracking the migration of the NCC towards FOC.

6.4.3.1.11. Is the central POC for network distribution and maintenance/update of Air Force Computer Emergency Response Team (AFCERT) and Automated Systems Security Incident Support Team (ASSIST) recommended security fixes, operating system patches, and antivirus software.

6.4.3.1.12. Maintains a data base of workload factor data depicting the number of network users, workstations, servers, and IP addresses as described in Air Force Manpower Standard (AFMS) 38DA. Also, include in this data base the building, room, POC, and phone number of the workload factor data. NCCs must be able to provide detailed reports in sorted formats as specified by the appropriate manpower office.

6.4.3.1.13. Manage routing protocols and base-wide domain name service.

6.4.3.1.14. NCCs perform minor application enhancement, software metering, backups,

recovery, and shuts down NM and system management systems when required.

6.4.3.1.15. Formats and partitions hard drives, performs file system management, and maintains boot service.

6.4.3.1.16. Provides assistance to SAs when needed and performs cryptographic equipment updates on devices under the control of the NCC.

6.4.3.1.17. Maintains selected equipment identified through SLAs or logistics support letters.

6.4.3.1.18. Distributes post regionalization Defense Management Review Decision (DMRD)-924 output product.

6.4.3.1.18.1. NCCs review/break down completed products, gather input material, and return items to the system analysis area.

6.4.3.1.18.2. Counts and certifies quantity of controlled products, operates decollators to separate carbon from printed product, reviews products for processing quality, and distributes to the appropriate bin for release to the customer.

6.4.3.1.19. Provides base network/NCC hardware/software installation service.

6.4.3.1.19.1. Hardware. NCCs install and configure network servers, routers, hubs, bridges, repeaters, servers, workstations, and peripherals. They test and document equipment installation acceptance testing.

6.4.3.1.19.2. Software. NCCs receive and inventory network software, test and validate new software applications and network operating systems (NOS).

6.4.3.1.19.2.1. Distribute and install network software releases and updates, and assist customers with software installation and customization.

6.4.3.1.19.2.2. Install network e-mail packages, InfoConnect, and TCP/IP software.

6.4.3.1.19.2.3. Install and configure SMTP hosts, relays, and gateways.

6.4.3.1.19.2.4. Review site license agreements and remove software from systems when no longer required or authorized.

6.4.3.1.20. Performs base NM planning.

6.4.3.1.20.1. NCCs maintain the base network characterization and validate the DISA Minimum Essential Circuit Listing (MECL) and the Defense Information Technology Contracting Office (DITCO) database product.

6.4.3.1.20.1.1. Collate local and long-haul customer telecommunications circuit information.

6.4.3.1.20.1.2. Verify current network configurations against other agency data bases and forward corrections as required.

6.4.3.1.21. NCCs perform base-wide configuration standardization and interface engineering.

6.4.3.1.21.1. Prepare and update in-station system block diagrams, network maps, and

facility equipment listings; maintain network and facility configuration plans; perform minor network engineering; monitor management information base (MIB) variables; and advise and make recommendations on new systems to customers.

6.4.3.1.21.2. Perform the following in conjunction with the base CSO and plans function:

6.4.3.1.21.2.1. Review project support agreements (PSA) and coordinate corrections with the appropriate agencies.

6.4.3.1.21.2.2. Coordinate with engineering and installation (EI) teams and/or commercial vendors prior to arrival and prepare the facility for installation team.

6.4.3.1.21.2.3. Escort and assist team chiefs with installation or upgrade projects.

6.4.3.1.21.2.4. Complete DD Form 250, **Material Inspection and Receiving Report**; AF Form 1261, **Command, Control, Communications, and Computer Systems Acceptance Certificate**; and EI critiques.

6.4.3.1.22. Prepares network migration and upgrade plans.

6.4.3.1.22.1. Coordinate with MAJCOM, ROSC, STEM-B, vendor, and/or contracting on network issues.

6.4.3.1.22.2. Evaluate new technology and incorporate upgrades into base network strategic plans.

6.4.3.1.23. Develops local restoral plan (LRP) and contingency operations plans.

6.4.3.1.23.1. NCCs research and determine requirements for maximum communications during contingency conditions.

6.4.3.1.23.2. Develop, test, and document implementation guidelines for base network communications contingencies from existing operations/war plans.

6.4.3.1.24. Processes requests and requirements for service.

6.4.3.1.24.1. NCCs perform impact assessments of C4 systems requirements document (CSRD), request for service (RFS), telecommunications service requests (TSR), status of acquisition messages (SAM), and telecommunications service orders (TSO).

6.4.3.1.24.2. Review, log-in, and research requests.

6.4.3.1.24.3. Provide technical advice and solutions for software, hardware, and network connectivity; assist in the preparation of AF Form 9, Request for Purchase, when required; create and maintain circuit layout records; update circuit and system labeling; complete in-house cross-connects and other minor device-to-demarcation point connections; and coordinate/perform initial test and acceptance on circuits.

6.4.3.1.24.4. Submit in-effect, exception, or delayed service reports as required, and develop and maintain a network circuit data base and network circuit history folders.

6.4.3.1.25. Performs automated data processing equipment (ADPE) equipment custodian (EC) duty.

6.4.3.1.25.1. NCCs verify receipt of equipment, perform audit, resolve and report known discrepancies.

6.4.3.1.25.2. Update the Information Processing Management System (IPMS) data base as required.

6.4.3.1.25.3. Issue equipment, perform initial and annual equipment inventory, and print and distribute inventory products.

6.4.3.1.25.4. Complete annual base-wide recertifications by account, monitor and assist unit ECs in ADPE responsibilities, monitor status of reports of survey, prepare reports of excess equipment, and complete paperwork for equipment turn-in.

6.4.3.1.25.5. Determine repair cost-effectiveness and submit cost estimate for equipment maintenance, process and monitor AF Forms 9 in conjunction with the plans function, maintain a software library, and destroy excess commercial software.

6.4.3.1.25.6. Issue loaner equipment if available, set up and delete customer accounts, and provide EC training.

6.4.3.1.26. Performs contract management for base network support.

6.4.3.1.26.1. NCCs consolidate and evaluate base-wide NCC-managed network and system components as candidates for contract maintenance support.

6.4.3.1.26.2. Submit inputs to the unit plans function for statement of work development.

6.4.3.1.26.3. Assist the plans function in the preparation of quality assurance surveillance plans (QASP) and perform contract quality assurance evaluation (QAE) functions as identified.

6.4.3.1.27. Performs base network budget planning.

6.4.3.1.27.1. NCCs develop/submit budget input and request higher-level funding for all NCC requirements and operations functions.

6.4.3.1.27.2. Monitor base network funds availability and process International Merchant Purchase Authorization Card (IMPAC) requests for hardware and software purchases following CSRD approval.

6.4.3.2. Fault Management:

6.4.3.2.1. Dispatches NCC or systems flight technicians to unmanned or user and subscriber locations when required to test, trouble-shoot, and restore service.

6.4.3.2.2. Coordinates with job control subscribers, local and distant support agencies, and contractors to isolate faults, restore service, and make repairs.

6.4.3.2.3. Ensures a trouble-call process is established for each IS.

6.4.3.2.4. SAs monitor difficulty reports, heads-up messages, and system advisory notices.

6.4.3.2.5. Provides network and small computer maintenance support.

6.4.3.2.6. Maintains LRU stock level and assist users in ordering replacement LRUs.

6.4.3.2.7. Provides technical support to SAs when requested and maintains an electrostatic discharge maintenance area.

6.4.3.2.8. Performs fault isolation to the LRU and line item equipment level. Fault isolation methods include automated diagnostics and sound trouble-shooting techniques.

6.4.3.3. Performance Management:

6.4.3.3.1. Coordinates installation, acceptance testing, QA, fault isolation, and restoration of the infrastructure with the base's other communications unit functions.

6.4.3.3.2. Establishes individual circuit and system parameters on non-DCS circuits. Develops the parameters according to DISAC 300-175-9, *DCS Operating Maintenance Electrical Performance Standards*, supplemented by commercial-leased equipment and circuit performance standards.

6.4.3.3.3. Establishes initial performance thresholds according to systems and circuit operation specifications and operational or mission requirements.

6.4.3.3.4. Integrates, configures, tests, monitors, analyzes, controls, and restores systems to maintain top performance of the base infrastructure and local support for DMC/RPC services.

6.4.3.3.5. Consolidates network performance data, security data, and analysis reports from all levels of the Air Force NM hierarchy. Uses the consolidated information to identify causes of service, performance, and security flaws. On the basis of the aggregated analysis, recommends changes in network configurations, hardware or software, procedures, and staff training.

6.4.3.3.6. Remotely tests subscriber equipment, end-to-end circuits, systems, and networks to verify the services provided and input and output signals meet standards.

6.4.3.3.7. Adjusts remote network element equipment to optimize service.

6.4.3.3.8. Records configuration data, test data, failure symptoms, coordination efforts, fault isolation steps performed, and any other useful information. Uses this information to evaluate and control operations, service capabilities, and service quality.

6.4.3.3.9. Reports to management on quality of infrastructure services.

6.4.3.3.10. Performs system diagnostics and sets global alarm thresholds and system parameters.

6.4.3.3.11. Monitors and optimizes network performance.

6.4.3.3.11.1. Establish circuit and system parameters for non-Defense Communication System circuits.

6.4.3.3.11.2. Utilize NM performance tools to ensure optimum network operation, monitor system logs, analyze bandwidth utilization, and set global parameters to prevent adverse affects to the overall communications network. Core systems must have critical path redundancy.

6.4.3.3.12. Performs network/circuit QC testing and evaluation.

6.4.3.3.12.1. Generate and update QC schedules.

6.4.3.3.12.2. Plan, provide, coordinate, and verify alternate service during QC testing.

6.4.3.3.12.3. Access and monitor preventative maintenance inspection (PMI) schedules published by the maintenance control workcenter.

6.4.3.3.12.4. Coordinate in-service/out-of-service QC testing and specific area support performance of PMIs with affected workcenters and external agencies.

6.4.3.3.12.5. Coordinate and deactivate alternate service once testing/PMIs are completed and original circuit/equipment is verified operational.

6.4.3.3.12.6. Analyze QC performance trend analysis data (collected through NMS or out-of-service QC testing) to identify trends or patterns of circuit/system/network degradation, dispatch to and from user locations when required, and generate and analyze outage reports.

6.4.3.3.12.7. Submit DD Form 1368, **Modified Use of Leased Communication Facilities**, when required, and research, prepare, and submit QC waiver requests when necessary, in the absence of a systems control facility.

6.4.3.4. Security Management:

6.4.3.4.1. Assists the wing IP office in developing a base-wide network security policy to effectively manage the base or wing networks. The NCC may request wing IP office assistance when developing a network security plan for the base backbone.

6.4.3.4.1.1. Terminate service and/or network connectivity of local systems and networks that fail to maintain compliance with Air Force and local security policy.

6.4.3.4.2. Assists the wing IP office in collecting accreditation information for base networks and systems. Ensures all systems and networks meet Air Force and local security requirements and have appropriate DAA approval before connecting to the base network infrastructure. Maintains historical documentation of all network and systems accreditation packages.

6.4.3.4.3. Conducts IPO according to AFPD 33-2, *Information Protection*, the AFI 33-200 series, and the specialized security publications prescribed in AFI 33-206, *Air Force Specialized Information Protection Publications*. Performs vulnerability assessments to test and validate security of networks and systems. If vulnerabilities are discovered, provides appropriate systems administrators, unit commanders, DAA, wing and MAJCOM IP offices, and AFCERT with test results and recommendations. Reports vulnerabilities found according to AFSSI 5021, *Vulnerability and Incident Reporting.*

6.4.3.4.4. Identifies weak configurations and security holes by auditing and monitoring events occurring on the network.

6.4.3.4.5. Conducts daily traffic analysis, identifies and characterizes incidents, and generates incident reports with Air Force approved intrusion detection tools. Investigates each item to clarify and resolve suspicious activity. Reports validated suspicious activity in according to AFSSI 5021.

6.4.3.4.6. Monitors audit and error logs for security violations and misuse.

6.4.3.4.7. Develops local procedures to report and respond to ISs and network stand-alone

computer security and virus incidents according to AFSSI 5021. Works with the wing IP office to identify internal actions such as local reporting channels, criteria for determining who is notified, etc.

6.4.3.4.8. Ensures all network users are aware the NCC has the technical means available to monitor, capture, and record/store all transmissions traversing its network (see AFI 33-219, *Telecommunications Monitoring and Assessment Program [TMAP]*).

6.4.3.4.9. Tests and validates network security to establish and maintain a target baseline for Air Force owned systems.

6.4.3.4.10. Installs and sets up audit tools, and coordinates with global, regional, and wing IP offices.

6.4.3.4.11. Executes automated scripts to test vulnerabilities and executes vulnerability procedures where no scripts are available (Network File System [NFS], Network Information System [NIS], cracking password, etc.). On systems accessed, NCCs test configuration for vulnerabilities.

6.4.3.4.12. Collects data on intrusion activity and intrusion reporting by SA and user.

6.4.3.4.13. Assists the SA to implement countermeasures and firewall systems on targeted systems.

6.4.3.4.14. Notifies users and SAs when their computers have weak configurations, vulnerabilities, and when they have been accessed, exploited, or destroyed by unauthorized persons or machines.

6.4.3.4.15. Reviews ASSIST vulnerability bulletins and AFCERT advisories, and verifies systems under NCC control are protected against documented vulnerabilities.

6.4.3.4.16. Performs certification and accreditation according to AFSSI 5024, Volume I, *The Certification and Accreditation (C&A) Process*, for ISs owned by the NCC.

6.4.3.4.17. Maintains automated security incident historical transaction tapes and logs.

6.4.3.4.18. Determines what data has been read, changed, or destroyed by unauthorized persons or machines.

6.4.3.4.19. Identifies and secures computer systems on an affected network. Identifies computers with exploited vulnerabilities.

6.4.3.4.20. Tests for signs of hacker activity on base network systems. Informs SAs and users on new systems security practices to prevent similar occurrences.

6.4.3.4.21. Briefs incidents as required by applicable AFIs, AFCERT advisories, and AFSSIs. Provides technical support as requested.

6.4.4. HD:

6.4.4.1. Monitors NM and system management system equipment.

6.4.4.1.1. Log on and off NM and system management systems.

6.4.4.1.2. Categorize, isolate, and resolve network problems.

6.4.4.1.3. Perform status checks and acknowledge alarm, generate NM and system

management systems reports, and maintain operational data base.

6.4.4.1.4. Monitor HD e-mail account and voice mail system, perform ad hoc queries, and coordinate and respond to Air Force, DISA, and Joint monitoring centers' directions.

6.4.4.2. Processes trouble calls and coordinates problem resolution.

6.4.4.2.1. Process and document customer trouble calls, monitor trouble ticket status, maintain trouble ticket data base, and create trouble ticket status reports.

6.4.4.2.2. Perform fault isolation by validating, isolating, and correcting faults, and verify service restoral with customers.

6.4.4.3. Processes scheduled and authorized outages (AO).

6.4.4.3.1. Review AOs to determine base network service impacts and coordinate with local users, prepare and submit AO messages, review responses, and maintain AO schedules.

6.4.4.3.2. Perform system checks after AOs are terminated.

6.4.4.4. Implements service restoral plans.

6.4.4.4.1. Authenticate restoral requests and implement required actions, verify service restoral, and coordinate completion of restoral plans with appropriate agency.

6.4.4.5. Prepares and submits formatted and unformatted reports.

6.4.4.5.1. Verify and submit required USAF and DISA reports on DCS hazardous conditions (HAZCON) and major communications outages according to DISAC 310-55-1, *Status Reporting for the Defense Communications Systems.*

6.4.5. FSA:

6.4.5.1. Complies with the policies of this instruction and maintains certification. Performs the functions defined for all NM areas and also assumes responsibilities delegated by the NCC or CSO to optimize communication infrastructure performance and quality of service. Consolidates systems administration duties within an organization or a building, if possible, merging them with the NCC based on an SLA.

6.4.5.2. Ensures servers, workstations, peripherals, communications devices, and operating system/application software are properly configured for network operation, are on-line, and are available to customers.

6.4.5.3. May also perform NM duties in which case the base network infrastructure components may be included. Paragraph **3.1.2.1.5.** contains a description of FSA duties and responsibilities.

6.4.5.4. Establishes contingency procedures, such as manual backup, reallocation of resources, and sharing assets, for systems critical to mission accomplishment.

6.4.5.5. Periodically reviews the organization's needs for computer resources.

6.4.5.6. Configures the operating system software to meet user needs (e.g., assigning user profiles, defining printer or modem access, and setting up user restrictions).

6.4.5.7. Defines ownership of applications and determining who has permission to read,

write, and execute.

6.4.5.8. Assigns and maintains userIDs and passwords IAW AFSSI 5013, *Identification and Authentication* (will convert to AFMAN 33-223), and administers user privileges on the system (e.g., which users share files).

6.4.5.9. Plans for short-term and long-term loss of system hardware and software. In configuring the system, the FSA and network security manager must decide on contingency plans in case of the FSA's absence. This may involve having another FSA administer the system remotely.

6.4.5.10. Monitors the network and the efficiency of the system (e.g., finding and resolving system bottlenecks).

6.4.5.11. Performs routine system maintenance such as backing up or archiving files and adding software updates.

6.4.5.12. Serves as the system trouble-shooter, a critical role in keeping the system operational. Contacts the NCC for hardware maintenance when necessary.

6.4.5.13. Works with the NCC and organizational computer systems security officers (CSSO) to implement network security policies and procedures as outlined in the systems security authorization agreement (SSAA), previously known as the accreditation package.

6.4.5.14. Ensures user training is conducted. Contacts the NCC for additional assistance.

6.4.5.15. Provides user manuals that include sign-on and sign-off procedures, use of basic commands, software policies, user responsibilities, etc.

6.4.5.16. The FSA's includes the user's terminal and the corresponding servers, but does not include the base network backbone infrastructure components. Some overlapping of responsibilities will occur.

6.4.5.16.1. Maintain access control to the network, and add, remove, and modify user profiles.

6.4.5.16.2. Submit templates upon activation, register with the Network Information Center (NIC), and request terminal access controller (TAC) access user cards.

6.4.5.16.3. Manage the message transfer agent (MTA), the message store, and the directory service agent (DSA).

6.4.5.16.4. Monitor daily e-mail activity and create and update NCC-controlled mail lists in the directory.

6.4.5.16.5. Operate post regionalization (DMRD-924) Data Communications Processor (DCP)-40/50 front-end-processors, coordinate and provide media conversions, and provide distributed print management.

6.4.5.16.6. Distribute standard and base level software release documents to users.

6.4.5.16.7. Maintain electronic bulletin boards and World Wide Web (WWW) home pages established by the NCC.

6.4.5.16.8. Count and certify quantity of controlled products and distribute output products.

6.4.5.16.9. Manage LAN and metropolitan area network (MAN) directories; add, remove, and modify directory service; verify directory synchronization; and maintain the master data base.

6.4.5.16.10. Download and distribute bulletin board information.

6.4.5.17. Implements software patches and security fixes as required by the NCC, NOSC, AFCERT, AFNOC, or program manager. Tests and validates the proper operation and configuration with appropriate patches and fixes, as required above, prior to restoring any device to the network.

6.4.6. Workgroup Manager (WM):

6.4.6.1. Complies with the policies of this instruction and maintains WM certification.

6.4.6.2. Complies with FSA and NCC policies.

6.4.6.3. Performs the installation of equipment, connection of peripherals, and the installing/ deleting of user software.

6.4.6.4. Configures user software, modifies software configuration, and performs basic configuration management functions.

6.4.6.5. Sets up and modifies user introduction menus.

6.4.6.6. Performs bulk-loading/updating data base files for resident application programs.

6.4.6.7. Performs database recovery for resident application programs.

6.4.6.8. Provides limited software application assistance for commonly used office automation applications purchased from standard Air Force infrastructure support contracts.

6.4.6.9. Performs e-mail address group maintenance, creating, modifying, and deleting directories, moving files from one media to another, and checking files for corruption.

6.4.6.10. Performs initial system diagnostics and trouble-shooting of systems assigned to them.

6.4.6.11. Formats, partitions, backs-up and restores hard drives.

6.4.6.12. Creates floppy boot disks.

6.4.6.13. Assigns, modifies, and deletes passwords and user privileges according to AFSSI 5013.

6.4.6.14. Reports security breaches, distributes security information, and assists in the development and maintenance of the SSAA.

6.4.6.15. Sends properly documented computer requirements to the base CSO for action.

6.4.6.16. Coordinates support issues with all agencies (e.g., customers, FSA, NCC, etc.).

6.4.6.17. Notifies the unit ADPE EC of any hardware relocation.

6.4.6.18. Obtains an implementation checklist from the MAJCOM, CSO, NCC, and FSA, before installing equipment. Assists with installing, testing, and accepting the system according to the terms of the purchase contract and instructions.

6.4.6.19. Isolates and resolves organization computer problems within own abilities, the FSA,

and applicable service contract before seeking assistance from the NCC.

6.4.6.20. Informs the accountable ADPE EC of computer equipment problems.

6.4.6.21. Coordinates with the facility manager and the base civil engineer for facility support requirements.

6.4.6.22. Documents technical support requirements on AF Form 332, **Base Civil Engineer Work Request**; and DD Form 1391, **FY____ Military Construction Program**. ***NOTE:*** More information on technical support requirements is available from the CSO and base contracting officer.

6.4.6.23. Periodically reviews the organization's needs for computer resources.

6.4.6.24. Identifies training and manpower issues and/or needs.

6.4.6.25. Documents integration and interoperability deficiencies and requests help from the CSO. ***NOTE:*** The CSO, through its plans flight, will assist the user to resolve integration/ interoperability problems.

6.4.6.26. Validates computer equipment requirements the unit EC submits.

6.4.6.27. When requested, assists the unit EC with computer hardware and software inventories.

6.4.6.28. Works with the FSA to ensure NM procedures comply with contracting documents.

6.4.6.29. Contacts the NCC for related information.

6.4.6.30. Sends all software with documentation costing more than $5,000, or requiring more than 40 man-hours to develop, to the base CSO for inclusion in the Defense Information Support Tool and possible use or reuse by other organizations.

6.4.6.31. Ensures the organization develops and maintains software according to MAJCOM guidance.

6.4.6.32. Reports computer resources to the organization EC at least 120 days prior to the equipment becoming excess.

6.4.6.33. Promotes user awareness concerning unauthorized or illegal use of computer hardware and software.

6.4.6.34. Identifies organization deficiencies and operational needs that computer use can solve.

6.4.6.35. Plans support for deployments (see AFIs 10-403, *Deployment Planning*; and 33-104, *Base-Level Planning and Implementation*).

6.4.6.36. Notifies the CSO of maintenance requirements for computers.

6.4.6.37. Establishes maintenance reporting procedures according to instructions provided by the CSO.

6.4.6.38. Ensures organizations do not use shareware or public domain software until approved for use by the DAA after the CSSO, WM, or FSA ensures it is free of viruses, hidden defects, and obvious copyright infringements.

6.4.6.39. Ensures organization shareware users pay any necessary fees.

6.4.6.40. Ensures correct management of records created by or stored on computers by coordinating with the unit records manager. These records include information for official use only or information subject to the *Privacy Act of 1974*. AFMAN 37-123, *Management of Records* (will convert to AFMAN 33-323), gives details on records management for computers. AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339), tells how to dispose of records.

7. Training .

7.1. Constant change in systems hardware and software capabilities, and high levels of service quality expected by users, require an in-depth training and certification program. All military and civilian network managers, systems administrators, and WMs will maintain certification defined at the local level on the most prevalent, preferred Air Force operating systems dependent on duties and responsibilities assigned.

7.2. Work with MAJCOM or AFCA to create and modify local and training base and MAJCOM modules and learning guides as you install or modify systems and services, and when you receive initial contractor training. The training modules and learning guides should conform to instructional systems development standards. They should qualify entry-level personnel to perform tasks as journeymen and supervisors and should support follow-on qualification training and certification. Elevate new Air Force training requirements to the appropriate MAJCOM AFSC functional manager. MAJCOM functional managers identify delta training requirements to the Air Force career field manager.

7.2.1. Do not modify nor eliminate training modules and learning guides just because all assigned personnel are currently qualified.

7.2.2. Use AFI 36-2201, *Developing, Managing, and Conducting Training*, to guide training program development, implementation, and maintenance.

7.3. Reduce the need for local training modules or learning guides by using Air Force on-the-job training products (see Air Force Index [AFIND] 8, *Numerical Index of Specialized Education/ Training Publications*). If existing Air Force job qualification standards or qualification training packages are not adequate, supplement them with local guides.

7.4. NCC personnel must receive both general and technical information protection training. General training provides knowledge of standard network threat and vulnerabilities, and standard security principles. Technical training qualifies individuals to implement specific information protection measures on the many different operating systems and security applications in use at a base. Obtain training either from the Air Education and Training Command (AETC) formal courses, through available distance learning training, or on-the-job training products.

7.5. Use all possible avenues of training delivery to achieve and maintain quality of service. AETC resident and field training detachment courses may not provide all the training needed at every location in the Air Force. Fill the gaps with computer-based training, commercial training, and unit-sponsored seminars and courses. People who attend commercial training courses should develop training modules and learning guides. Keep all commercial course materials and use them to deliver follow-on training.

7.6. NCCs must ensure NM support personnel subordinate to the NCC (i.e., FSA and WM) receive adequate training prior to performing duties in any area.

7.7. NCCs provide education and training to base computer users.

7.7.1. Ensure operators, WMs, and FSAs receive a level of instruction commensurate with their duties and responsibilities.

7.7.2. Draft and forward customer education letters or handbooks, conduct customer training surveys, and advertise training availability.

7.7.3. Prepare training outlines and course material, train instructors, prepare class schedules, schedule customers for training, configure computers for specific courses, and conduct customer training classes.

7.7.4. Conduct evaluations to see if training meets the customers needs and develop and maintain a base reference library for hardware and software applications.

7.7.5. Educate functional systems administrators, WMs, and other base customers in network services, fault isolation, security, and trouble reporting.

7.7.6. Visit user organizations to stay familiar with user requirements.

7.7.7. Security awareness training will be provided in accordance with AFI 33-204, *Security Awareness, Training, and Education*.

8. Checklists . Use the questions at **Attachment 5**, along with AF Form 2519 (available electronically), to develop a checklist on NCC QA. Use it to perform self-inspections, staff assistance visits, and performance evaluations.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCSM 6231.07A, (FOUO) *Manual for Employing Joint Tactical Communications Systems - Joint Network Management and Control,* January 1995

DISAC 310-55-1, *Status Reporting for the Defense Communications Systems*

DISAC 300-175-9, *DCS Operating Maintenance Electrical Performance Standards*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFI 10-403, *Deployment Planning*

AFI 33-104, *Base-Level Planning and Implementation*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-129, *Transmission of Information Via the Internet*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFI 36-2201, *Developing, Managing, and Conducting Training*

AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* (will convert to AFI 33-324)

AFIND 8, *Numerical Index of Specialized Education/Training Publications*

AFMAN 37-123, *Management of Records* (will convert to AFMAN 33-323)

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339)

AFSSI 4100, (C) *Communications Security Program (U)*

AFSSI 5013, *Identification and Authentication* (will convert to AFMAN 33-223)

AFSSI 5021, *Vulnerability and Incident Reporting*

AFSSI 5024, Volume I, *The Certification and Accreditation (C&A) Process*

Base Network Control Center Concept of Operations (CONOPS)

Abbreviations and Acronyms

ADPE—Automated Data Processing Equipment

AETC—Air Education and Training Command

AF—Air Force (used for forms only)

AFCA—Air Force Communications Agency

AFCERT—Air Force Computer Emergency Response Team

AFFOR—Air Force Forces

AFGWC—Air Force Global Weather Central

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMS—Air Force Manpower Standard

AFNOC—Air Force Network Operations Center

AFPD—Air Force Policy Directive

AFSC—Air Force Specialty Code

AFSSI—Air Force Systems Security Instruction

AO—Authorized Outage

AOR—Area of Responsibility

ASSIST—Automated Systems Security Incident Support Team

AUTODIN—Automated Digital Network

BIP—Base Information Protection

C2—Command and Control

C4—Command, Control, Communications, and Computer

CINC—Commander in Chief

CONOPS—Concept of Operations

CONUS—Continental United States

CSO—Communications and Information Systems Officer

CSSO—Computer Systems Security Officer

CSRD—C4 Systems Requirements Document

CSU—Channel Service Unit

DAA—Designated Approval Authority

DCP—Data Communications Processor

DCS—Defense Communications System

DD—Department of Defense (used for Forms only)

DHCP—Dynamic Host Configuration Protocol

DII—Defense Information Infrastructure

DIICC—Defense Information Infrastructure Control Concept

DISA—Defense Information Systems Agency

DISAC—Defense Information Systems Agency Circular

DISN—Defense Information Systems Network

DITCO—Defense Information Technology Contracting Office

DMC—Defense Megacenter

DMRD—Defense Management Review Decision

DMS—Defense Message System

DNS—Domain Name System

DoD—Department of Defense

DSA—Directory Service Agent

DSCSOC—Defense Satellite Communications System Operations Center

DSU—Digital Service Unit

EI—Engineering and Installation

e-mail—Electronic Mail

FCO—Facility Control Office

FOC—Final Operational Capability

FSA—Functional System Administrator

GCCS—Global Command and Control System

GMC—GCCS Management Center

GOSC—Global Operations and Security Center

GPS—Global Positioning System

HAZCON—Hazardous Condition

HD—Help Desk

IMPAC—International Merchant Purchase Authorization Card

IP—Internet Protocol

IPO—Information Protection Operations

IPMS—Information Processing Management System

IS—Information System

JCCC—Joint Communications Control Center

JTF—Joint Task Force

LAN—Local Area Network

LCC—Local Control Center

LRP—Local Restoral Plan

LRU—Line Replaceable Unit

MAN—Metropolitan Area Network

MAJCOM—Major Command

MECL—Minimum Essential Circuit Listing

MEDSITE—Medical Systems Implementation and Training Element

MIB—Management Information Base

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

MTA—Message Transfer Agent

NA—Network Administration

NAT—Network Address Translator

NCC—Network Control Center

NDS—Network Directory Service

NFS—Network File System

NIC—Network Information Center

NIPRNET—Non-Classified Internet Protocol Router Network

NIS—Network Information System

NM—Network Management

NMS—Network Management System

NOS—Network Operating System

NOSC—Network Operations and Security Center

NTP—Network Time Protocol

OPSEC—Operations Security

O/PTN—Operationalize and Professionalize the Network

PC—Personal Computer

PMI—Preventative Maintenance Inspection

POC—Point of Contact

PSA—Project Support Agreement

PSCF—Primary Systems Control Facility

QA—Quality Assurance

QAE—Quality Assurance Evaluation

QASP—Quality Assurance Surveillance Plan

QC—Quality Control

ROSC—Regional Operations and Security Center

RFS—Request for Service

RPC—Regional Processing Center

SA—System Administrator

SAM—Status of Acquisition Messages

SDP—Service Delivery Point

SIPRNET—SECRET Internet Protocol Router Network

SLA—Service Level Agreement

SMTP—Simple Mail Transfer Protocol

SNMPv1—Simple Network Management Protocol Version 1

SSAA—Systems Security Authorization Agreement

STEM-B—Systems Telecommunications Engineering Manager - Base Level

STEM-C—Systems Telecommunications Engineering Manager - Command Level

SYSCON—Service Systems Control

TAC—Terminal Access Controller

TCP/IP—Transmission Control Protocol/Internet Protocol

TSO—Telecommunications Service Order

TSR—Telecommunications Service Request

WAN—Wide Area Network

WM—Workgroup Manager

WWW—World Wide Web

Attachment 2

CLASSES OF NETWORK ELEMENTS

A2.1. Networks formed by element classes support the conversion, storage, processing, and transfer of audio, video, text, and graphics information. The information is shared within and between workgroups, organizations, buildings, and bases.

A2.2. General classes of network elements making up the base-level communications and information infrastructure that are managed by the Air Force NM hierarchy are:

A2.2.1. Human/machine interface.

A2.2.2. Telephone.

A2.2.3. Facsimile.

A2.2.4. Video.

A2.2.5. Application programs.

A2.2.6. Computer operating systems.

A2.2.7. NOSs.

A2.2.8. Communications protocols.

A2.2.9. Computer/workstation systems.

A2.2.9.1. Personal.

A2.2.9.2. Multi-user.

A2.2.9.3. Mini.

A2.2.9.4. Mainframe.

A2.2.9.5. Front-end processor.

A2.2.10. Specialized input/output devices.

A2.2.10.1. Printers.

A2.2.10.2. Plotters.

A2.2.10.3. Scanners.

A2.2.10.4. Computer-controlled presentation systems.

A2.2.10.5. Session encryption devices.

A2.2.10.6. Access control devices.

A2.2.10.7. Back-up devices.

A2.2.10.8. Mass storage (RAID).

A2.2.10.9. Pointer and drawing devices.

A2.2.10.10. Tactile sensors.

A2.2.10.11. Voice control devices.

A2.2.10.12. CD-ROMs.

A2.2.11. Access switches.

A2.2.12. Matrix switches.

A2.2.13. Packet switches (packet assemblers/dissemblers).

A2.2.14. Stored program circuit switches.

A2.2.15. Concentrators.

A2.2.16. LAN/WAN.

A2.2.16.1. LAN server processors (including disk, file, applications, and servers).

A2.2.16.2. Network interface cards.

A2.2.16.3. Protocol converters.

A2.2.16.4. Hubs.

A2.2.16.5. Transceivers.

A2.2.16.6. Media access units.

A2.2.16.7. Bridges.

A2.2.16.8. Routers.

A2.2.16.9. Gateways.

A2.2.16.10. Link encryption devices.

A2.2.17. Smart multiplexers.

A2.2.18. Modem/line drivers.

A2.2.19. Digital access and cross-connect systems.

A2.2.20. Multiplexer.

A2.2.21. Media (media drivers).

A2.2.22. Firewalls.

A2.2.23. In Line Encryptors (INE).

Attachment 3

SAMPLE SERVICE LEVEL AGREEMENT CONTENT AREAS

The following is a sample of a SLA format between the service provider (NM location) and the customer. The sample agreement only shows minimum topics that should be addressed:

1. Introduction. Parties (organizations) involved:

   a. Service provider: (i.e., DAA or NCC).

      (1) POC names.

      (2) Location or office symbol.

      (3) Telephone numbers.

   b. End-user organization.

      (1) POC names.

      (2) Location or office symbols.

      (3) Telephone numbers.

2. Purpose. The purpose of this SLA is to state the relationship between the service provider and the end-user organization. It specifies the services and commitments of the NCC as well as the expectations and obligations of the end-user organization.

3. Responsibilities of Service Provider (Name of the Organization). The service provider agrees that it will:

   a. Specify what resources it will use.

   b. Describe how they will inform the customer of infrastructure changes and new or changed service.

   c. State security methods that they will use to protect infrastructure resources from unauthorized access, monitoring, or tampering.

   d. Describe process used to notify and coordinate with end-user organization about planned outages of connectivity, equipment, or electricity.

   e. Explain the coordination process for service degradation or failure correction and state how customer will be kept informed of status.

   f. Describe materials that will be provided to customer to minimize procedural errors.

   g. Explain customer support performance criteria and workload limitations (for example, hours of operation, response times, expected maximum calls).

   h. Describe what performance data and analysis reports they will provide to the customer organization to show service quality and level of customer support provided.

   i. State what customer training is available and what role the service provider's will play in customer training.

   j. Perform periodic surveys to monitor customer satisfaction.

k. State the security measures they will use to protect infrastructure resources from unauthorized access, monitoring, or tampering.

4. Responsibilities of End-User Organization.

a. The end-user organization agrees that it will:

(1) Describe the process used to ensure end-users know procedures for getting help.

(2) Coordinate with service provider on any major configuration changes (for example, network installation/expansion, TCP/IP port requirements, change in topology, system upgrades, relocation, and so forth).

(3) Describe the process used to notify end-users of planned outages of connectivity, equipment, or electricity.

(4) Workgroup managers and SAs will provide, upon request, equipment layout, network schematic, network connectivity (attached via backbone or stand alone), and their exact location.

(5) Describe how they will use the performance and trend analysis data from service provider and provide feedback to improve service.

(6) Develop end-user contingency operations plans and capabilities.

(7) Identify what resources they will matrix or transfer to the service provider.

(8) Provide service provider with access to equipment both electronically and physically as needed.

(9) Agrees to perform the certification effort and comply with wing or NCC security policy.

b. During a trouble call, the end users will:

(1) Contact end-user organization POC first, if available.

(2) Describe what minimum information they will provide (for example, name, organization, location, telephone number, equipment number, user-id, e-mail address).

(3) Provide service provider with a description of problem, it's priority, and potential mission impact.

(4) Work with the service provider during fault isolation process, as needed.

(5) Negotiate for increased workload/expansion d for contingencies or new support.

5. Customer Escalation Procedures. The two parties agree to the following procedures in case they need to escalate resolution of the problem (that is, when the customer is not satisfied with the service provided):

ESCALATION LEVELS	TO WHOM	PHONE NUMBER
1st		
2nd		
3rd		

6. Conclusion.

a. Parties agree that the terms of this agreement will remain in effect for (5 years, 6 months, and so forth) are subject to review (annually, semiannually, and so forth).

b. The parties agree to the following mechanism for initiating an out-of-cycle SLA review:

Service levels and procedures established herein were agreed to by parties represented by undersigned.

_____ _____

(Service Provider Representative Signature) (End-User organization Signature)

Attachments (add as needed):

1. Hours of Operation.
2. Definitions of Terminology.
3. Lists of Support Equipment and Software.
4. Summaries of Applicable Contracts.
5. Contingency Plan.

Attachment 4

SYSTEMS AND NETWORK SUPPORT

Table A4.1. identifies the breakdown of network elements, tasks performed, and assigns responsibility.

Table A4.1. Systems and Network Support Task Breakdown.

Classes of Network Elements	Tasks	NA/ FSA	NM	WM	End User	Wire Cable
Computer/Workstation Single Client Systems		X		X	X	
	Select operating area			X	X	
	Install equipment	X		X	X	
	Connect peripherals	X		X	X	
	System startup	X		X	X	
	Maintain hardware	X		X	X	
	Create, modify, delete directories	X		X	X	
	Construct file systems	X			X	
	Move files from one media to another			X	X	
	Review file contents	X		X	X	
	Secure files from erasure				X	
	Check files for corruption			X	X	
	Perform system diagnostics	X		X	X	
	Format, partition, repartition to determine available disk space	X				
	Format floppies				X	
	Create floppy boot disk			X	X	
	Make copies of floppies				X	
	Install, modify remove systems security	X		X	X	

	Backup and restore hard drives	X		X	X	
	Customize backup device driver	X		X	X	
	Recover from system crash	X		X		
	Physical security	X		X	X	
Multi-user Systems/ Server						
	Receive and inventory equipment	X		X		
	Select operating area	X				
	Install equipment	X	X			
	Install cabling	X	X			X
	System startup	X				
	Maintain hardware	X	X			
	Create, modify, delete directories	X				
	Construct file systems	X				
	Move files from one media to another	X		X		
	Review file contents	X		X		
	Secure files from erasure	X				
	Check files for corruption	X				
	Perform system diagnostics	X				
	Format, partition, repartition to determine available disk space	X				
	Format floppies	X		X		
	Create floppy boot disk	X		X		
	Make copies of floppies	X				

	Install, modify remove systems security	X				
	Backup and restore hard drives	X				
	Customize backup device driver	X				
	Recover from system crash	X				
	Physical security	X				
Client Workstation Resident Application Programs						
	Install and Delete user software			X	X	
	Customize user software			X	X	
	Diskless server support	X		X		
	Provide trouble shooting	X		X		
	Receive or inventory software			X	X	
	Install/configure software			X	X	
	Modify software configuration			X	X	
	Remove software			X	X	
	Set up and modify user interface menus	X		X	X	
	Bulk-loading and updating data base tables			X		
	Data base recovery			X		
	Customize error messages	X		X		
	E-mail/DMS address groups maintenance			X		
Specialized Devices						

	Install peripherals			X	X	
	Install routers		X			
	Install bridges		X			
	Install hubs/ concentrators		X			
	Media access units		X			
	Channel service unit (CSU)/Digital service unit (DSU)		X			
	Install cabling		X			
	Load network loadable modules	X				
	Implement access control	X	X			
	Add/remove users	X	X	X		
	Modify defaults used to add users	X				
	Modify user profiles	X		X		
	Change user system addresses	X	X			
	Backup systems (servers)	X				
	Audit activity	X	X			
	Provide trouble-shooting	X	X	X		
	Monitor system per-formance	X	X			
	Monitor and clear system logs	X				
	Advise users to remove unnecessary files	X		X		
	Customize login process	X				
Network Applications						
	Develop network menuing system	X				
	Load license and metering applications	X				
	Virus scanning	X				

	E-mail	X				
	Receive/inventory network applications	X				
	Install/configure, modify network application software	X				
	Directory services	X				
Network Management						
	Install NM system		X			
	Install NM software		X			
	Physical NM	X	X			X
	Mapping network devices	X	X			
	Cable management		X			X
	Utilize protocol analyzer		X			
	Utilize network monitor	X	X			
Security Management						
	Authorizing users	X	X	X		
	Examining security logs	X	X			
	Performing risk analysis	X	X	X		
	Performing Vulnerability Assessments		X			
Performance Management		X	X			
	Gathering network statistics	X	X			
	Examining network history logs	X	X			
	Evaluating systems performance under normal/degraded conditions	X	X			
	Produce trend reports	X	X			
	Trend analysis	X	X			

	Traffic analysis (SNMP)		X			
Configuration Management		X				
	Setting parameters	X	X			
	Changing network configuration	X	X			
	Moves, adds, changes	X	X	X		
	Remote management	X	X			
	Router management		X			
	Load routing tables		X			
	Bridge management		X			
	Problem tracking	X	X	X		
	IP address management		X			
	Data switch/TAC		X			
	Audit activity	X	X			
	Provide trouble-shooting	X	X	X		X
Fault Management						
	Fault recognition	X	X	X	X	
	Fault diagnosis	X	X	X		
	Fault bypass recovery	X	X			
	Fault tracking and control	X	X			
	Integrate LANs to WAN	X	X			
	Communication test procedures	X	X			
	Network architecture	X	X			
	Quality assurance	X	X			
	Trouble database maintenance	X	X			
	Future planning/ technology insertion	X	X	X	X	X

NA = Network Administration
FSA = Functional Systems Administrator
Net Mgt = Network Management
WM = Workgroup Manager
Wire/Cable = Physical Management of the Cable and Wire of the network

Attachment 5

QUALITY ASSURANCE

Use the following questions to develop a NCC checklist. This attachment identifies the roles and responsibilities of the various functional areas that work with the NCC. Use it to perform self-inspections, staff assistance visits, and performance evaluations. Augment these questions as needed using the necessary local, MAJCOM, or Air Force directives.

Base Communications and Information Systems Officer:

1. Has the base CSO identified NM requirements to support NM functions that the wing, base, or unit are tasked for operations and sustainment? (**6.3.1.**)

2. Has the base CSO identified requirements to establish specific community of interest NM capabilities in support of operational or new missions that they cannot provide with existing NCC resources? (**6.3.1.**)

3. Does the base CSO work with the STEM-B and STEM-C to define and integrate technical solutions to the base blueprint for funding prioritization and future implementation? **6.3.1.**)

4. Does the base CSO use Air Force 33-series publications and negotiated support agreements to imbed centralized NM support requirements and concepts in performance work statement definitions during initial, renegotiated, or amended contracting actions (base contracts)? (**6.3.2.**)

5. Has the base CSO allocated to each NM area enough resources to meet service provisioning response times, service availability standards, service degradation or failure restoral times, user or subscriber education and training needs, network security monitoring and protection, on-line surveys, security incident reporting and response, network mapping, and deployment or contingency support requirements? (**6.3.3.**)

6. Has the base CSO established or consolidated a NM area subordinate to the NCC according to user or subscriber negotiated service level of agreements, system or network performance specifications, and minimum Air Force NM quality of service standards? (**6.3.4.**)

7. Has the base CSO established internal briefing and reporting requirements (frequency and format) for infrastructure status, performance, and quality of service to aid base-level decision-making regarding infrastructure changes, procedures, training, and other issues? (**6.3.5.**)

8. Does the base CSO support host and tenant organization missions? (**6.3.6.**)

9. Does the base CSO evaluate the services provided by each area NM location according to system or network performance standards? (**6.3.7.**)

10. Does the base CSO direct changes in procedure, allocation of resources, or training methods to minimize resource requirements and improve quality of service? (**6.3.7.**)

11. Has the base CSO established a wing steering group to develop base policy and procedures for migrating NM toward the Air Force architectures and standards? (**6.3.8.**)

12. Does the base CSO target stand-alone and redundant NM capabilities and responsibilities for consolidation to minimize the amount of resources used to do NM while optimizing performance and quality of service? (**6.3.9.**)

13. Does the base CSO report the findings to the wing level (or equivalent) steering group and the STEM-B for inclusion in the base blueprint? (**6.3.9.**)

Network Control Center:

1. Does the NCC perform the following network services according to established policy, SLAs, MOAs, and MOUs:

   a. Allocation and minor engineering.

   b. Installation.

   c. QC and QA.

   d. NM operations and security.

   e. Education and training. (**6.4.1.**)

2. Does the NCC remotely provide equivalent service for unmanned sites or facilities, when required? (**6.4.1.6.**)

3. Has the NCC established a HD function as the base's single POC for problems? (**6.4.1.7.**)

4. Does the NCC serve as local support for customers and systems of the DMS, DISN, RPCs, and community of interest areas in accordance with DISACs, negotiated support agreements, and the Air Force 33-series publications? (**6.4.1.8.**)

5. Does the NCC perform as contractor QA evaluator for NCC-monitored service contracts? (**6.4.1.9.**)

6. Does the NCC support small and minicomputer hardware and software prescribed for the small computer systems element in AFI 33-112? (**6.4.1.10.**)

7. Does the NCC provide residual support for base standard base-level computer customers? (**6.4.1.11.**)

8. Does the NCC act as DISN node site coordinator as defined in DISAC P70-series and Air Force 33-series publications? (**6.4.1.12.**)

9. Does the NCC provide deployed systems and NM services as tasked by the wing commander? (**6.4.1.13.**)

10. Does NM use Air Force 33-series publications and applicable DoD, DISA, and USAF publications to govern and guide network operations? (**6.4.1.15.**)

11. Does NM participate in the Quality Air Force process, requirements technical solution evaluation process, interfunctional support negotiations, procedural definition process, and workgroups? (**6.4.1.16.**)

12. Does NM identify and defend, through the base CSO, resource and training requirements to optimize domain service delivery and capability, including support for deployment and contingency operations? (**6.4.1.17.**)

13. Does NM reallocate resources to higher levels, when possible? (**6.4.1.17.**)

14. Did the NCC establish performance and quality of service standards for each class of connection and service? (**6.4.1.18.**)

15. Does NM use DoD and USAF standards, unless more stringent standards are negotiated? (**6.4.1.18.**)

16. Does the NCC sponsor education and training seminars for users, subscribers, and infrastructure technicians? **6.4.1.19.**)

17. Did the NCC supplement material given in other training programs? (**6.4.1.19.**)

18. Does the NCC orient education toward improving the infrastructure quality of service and security? (**6.4.1.19.**)

19. Does the NCC train personnel to:

a. Allocate and configure services and resources.

b. Control quality of NM operations.

c. Administer security.

d. Administer data bases.

e. Certify training and positions.

f. Install systems.

g. Manage and respond to trouble calls.

h. Perform NM system operations (e.g., configuration, fault, performance, security, and accounting management).

i. Educate and train customers.

j. Perform LRU-level maintenance on network hardware (i.e., servers, PCs, routers, hubs, switches). (**6.4.1.20.**)

20. Has the NCC established a position certification program for each position within the organization? (**6.4.1.21.**)

21. Does NM gather and analyze performance data on services provided by the infrastructure domain or domains within the NM area's span of control? (**6.4.1.22.**)

22. Does the NCC enter data and analysis results onto an electronic bulletin board so that all levels of the Air Force NM hierarchy can use it? (**6.4.1.23.**)

23. Does NM recommend corrections for service problems (e.g., configuration or procedure changes, additional training, equipment upgrades, additional test devices)? (**6.4.1.22.**)

24. Does the NCC send MAJCOMs a copy of internally developed or modified procedures, agreements, process flowlists, checklists, informational handouts, and training materials for review, consolidation, and reissue by other USAF and DoD organizations? (**6.4.1.23.**)

25. Does the NCC develop, coordinate, and maintain support plans for contingency, service restoration, unit type code requirements, and deployed capability? Does the NCC validate and test plans regularly? (**6.4.1.24.**)

26. Does NM manage resources within a NM area's domain through automated processes for such things as permissions, scheduling, database administration, memory backups, and memory and file allocation? (**6.4.1.25.**)

27. Does NM implement, operate, and maintain appropriate security measures? (**6.4.1.26.**)

28. Does NM maintain, or have access to, a library of DoD, USAF, and MAJCOM publications, commercial manuals, training material, and technical orders for operations and maintenance of domain resources? (**6.4.1.27.**)

29. Does the NCC keep an inventory of base and long-haul telecommunications equipment? (**6.4.1.28.**)

30. Does the NCC develop and maintain network configuration maps and/or developed data base that documents the network infrastructure to include the number of servers and terminals supported? (**6.4.1.29.**)

Network Administration:

1. Does the NCC provide a suite of common services to its base customers? (**6.4.2.**)

2. Does the NCC configure, install, and manage the following data services as required, as well as any other additional services required by local policy and procedures? (**6.4.2.**)

3. Did the NCC acquire control of all base IP address space and do they manage it through utilization of DHCP, Bootp, or static configuration? (**6.4.2.1.**)

4. Once control was established, did the NCC introduce the NAT to support the IP boundary protection concept? (**6.4.2.1.**)

5. Has the NCC enabled DNS to eliminate the dependence on a centrally maintained file that maps host names to addresses? (**6.4.2.2.**)

6. Has the NCC enabled SMTP and AUTODIN services that will continue to be offered until all end-users migrate to a fully implemented and operational DMS? (**6.4.2.3.2.**)

7. Has the NCC provided a communications server capable of handling dial-in and dial-out services? (**6.4.2.4.**)

8. Is the server placed outside the BIP boundary to prevent the possibility of back-door access? (**6.4.2.4.**)

9. Does the NCC control all remote dial-in and dial-out communications services? (**6.4.2.4.**)

10. Has the NCC/wing developed a core set of supported applications? (**6.4.2.5.**)

11. Are HD personnel knowledgeable in the applications the wing supports? (**6.4.2.5.**)

12. Does the NCC provide software assistance support for the wing's core set of applications? (**6.4.2.5.**)

13. Is the NCC the focal point for providing all access to NIPRNET and the Internet? (**6.4.2.6.**)

14. Does the NCC provide a global naming service that maintains information on, and provides access to, every resource on the network, including users, groups, printers, volumes, and servers? (**6.4.2.7.**)

15. Does the NCC provide support to local customers using the DMC services? (**6.4.2.8.**)

16. Does the NCC provide print management (i.e., print and distribute listing for IS users without distributive print work-stations) to include print services within the NCC, remote distributed print services, and organizational network server printers for which the NCC has an SLA? (**6.4.2.8.**)

17. Does the NCC deny external NTP sources through the BIP boundary due to inherent security problems? (**6.4.2.9.**)

18. Does the NCC utilize NTP within the IP boundary protection to synchronize system clocks with a local GPS receiver? (**6.4.2.9.**)

19. Has the NCC developed methods to handle new network technologies as they develop? (**6.4.2.10.**)

Network Control Center Network Management

Configuration Management:

1. Does the NM control all communications service points on a base? (**6.4.3.1.1.**)

2. Does the NM make sure all service points have functional layout diagrams, hardware interconnection listings, test point location listings, and expected signal characteristics at each test point? (**6.4.3.1.1.**)

3. Does the NM ensure that the service points have hardware labels that clearly identify individual circuit connections and test points? (**6.4.3.1.1.**)

4. If the service point is too small to contain the above information, does the NM maintain copies for dispatch technicians to use? (**6.4.3.1.1.**)

5. Does the NM document any changes in the service point configuration or in service operation in the service point information? (**6.4.3.1.1.**)

6. Does the NM work with STEMs and participate in the review and planning of base transmission media and telecommunications systems networks? (**6.4.3.1.2.**)

7. Does the NM make sure replacements for legacy or dumb network devices incorporate remote support capability to improve centralized NM performance and quality? (**6.4.3.1.2.**)

8. Does the NM remotely perform the functions and duties of a DCS PSCF, patch and test facility, DCS switching center, or other DCS operations function, when it is technically and economically feasible and does not degrade quality of service in accordance with DISA procedures? (**6.4.3.1.3.**)

9. To support the wing during contingencies, does the NM take over the responsibility and authority of the PSCF for DCS service control? (**6.4.3.1.3.**)

10. Does the NM remotely configure user and subscriber terminals, computer hardware and software resources, intrabase and long-haul (tail) circuits, systems, and networks? (**6.4.3.1.4.**)

11. Does the NM document the base reconfiguration on subscriber service requirements, network traffic patterns and loading, and results of QA tests? (**6.4.3.1.4.**)

12. Does the NM extend from the interface of the user's terminal to the interfaces of the base-level host, base-level server, or transmission system providing connectivity to off-base assets and include all the base network backbone infrastructure components? (**6.4.3.1.5.**)

13. Does the NM reconfigure equipment or mode of operation by replacing, restrapping, or reprogramming circuit boards, modules, subassemblies, and assemblies? (**6.4.3.1.6.**)

14. Does the NM maintain, manage, control, and distribute the IP address space allocated to the base internet? (**6.4.3.1.7.**)

15. Does the NM establish, maintain, control, and enforce the base internet use policy? (**6.4.3.1.8.**)

16. Is the NM the central POC for network distribution and maintenance/update of AFCERT and ASSIST recommended security fixes, operating system patches, and antivirus software? (**6.4.3.1.11.**)

17. Does the NM maintain a data base of workload factor data depicting the number of networked users, workstations, servers, and IP addresses; the building, room, POCs, and phone numbers as described in AFMS 38DA? (**6.4.3.1.12.**)

18. Does the NM provide detailed reports in sorted formats as specified by the appropriate manpower office? (**6.4.3.1.12.**)

19. Does the NM manage routing protocols and base-wide domain name service? (**6.4.3.1.13.**)

20. Does the NM perform minor application enhancement, software metering, backups, recovery, and shutdown of NM and system management systems when required? (**6.4.3.1.14.**)

21. Does the NM format and partition hard drives, perform file system management, and maintain boot service? (**6.4.3.1.15.**)

22. Does the NM provide assistance to SAs when needed and perform cryptographic equipment updates on devices under the control of the NCC? (**6.4.3.1.16.**)

23. Does the NM maintain selected equipment identified through an SLA or logistics support letter? (**6.4.3.1.17.**)

24. Does the NM distribute the post regionalization (DMRD-924) output product? (**6.4.3.1.18.**)

25. Does the NM review/breakdown completed products, gather input material, and return items to the system analysis area? (**6.4.3.1.18.1.**)

26. Does the NM count and certify quantity of controlled products, operate decollators to separate carbon from printed product, review products for processing quality, and distribute to the appropriate bin for release to the customer? (**6.4.3.1.18.2.**)

27. Does the NM provide base network/NCC hardware/software installation service? (**6.4.3.1.19.**)

28. Does the NM install and configure network servers, routers, hubs, bridges, repeaters, servers, workstations, peripherals, etc.? (**6.4.3.1.19.1.**)

29. Does the NM test and document equipment installation acceptance testing? (**6.4.3.1.19.1.**)

30. Does the NM receive and inventory network software, test and validate new software applications and NOSs? (**6.4.3.1.19.2.**)

31. Does the NM distribute and install network software releases and updates, and assist customers with software installation and customization? (**6.4.3.1.19.2.1.**)

32. Does the NM install network e-mail packages, InfoConnect, and TCP/IP software? (**6.4.3.1.19.2.2.**)

33. Does the NM install and configure SMTP hosts, relays, and gateways? (**6.4.3.1.19.2.3.**)

34. Does the NM review site license agreements and remove software from systems when no longer required or authorized? (**6.4.3.1.19.2.4.**)

35. Does the NM perform base NM planning? (**6.4.3.1.20.**)

36. Does the NM maintain the base network characterization and validate the DISA MECL and the DITCO database product? (**6.4.3.1.20.1.**)

37. Does the NM collate local and long-haul customer telecommunications circuit information? (**6.4.3.1.20.1.1.**)

38. Does the NM verify current network configurations against other agencies' data bases and forward corrections as required? (**6.4.3.1.20.1.2.**)

39. Does the NM perform base-wide configuration standardization and interface engineering? (**6.4.3.1.21.**)

40. Does the NM prepare and update in-station system block diagrams, network maps, and facility equipment listings; maintain network and facility configuration plans; perform minor network engineering; monitor MIB variables; and advise and make recommendations on new systems to customers? (**6.4.3.1.21.1.**)

41. Does the NM review PSAs and coordinate corrections to the appropriate agencies? (**6.4.3.1.21.2.1.**)

42. Does the NM coordinate with EI teams and/or commercial vendors prior to arrival and prepare the facility for installation team? (**6.4.3.1.21.2.2.**)

43. Does the NM escort and assist team chiefs with installation or upgrade projects? (**6.4.3.1.21.2.3.**)

44. Does the NM complete DD Form 250, AF Form 1261, and EI critiques? (**6.4.3.1.21.2.4.**)

45. Does the NM prepare network migration and upgrade plans? (**6.4.3.1.22.**)

46. Does the NM coordinate with MAJCOM, ROSC, STEM-B, vendor, and/or contracting on network issues? (**6.4.3.1.22.1.**)

47. Does the NM evaluate new technology and incorporate upgrades into base network strategic plans? (**6.4.3.1.22.2.**)

48. Does the NM develop LRP and contingency operations plans? (**6.4.3.1.23.**)

49. Does the NM research and determine requirements for maximum communications during contingency conditions? (**6.4.3.1.23.1.**)

50. Does the NM develop, test, and document implementation guidelines for base network communication contingencies from existing operations/war-plans? **6.4.3.1.23.2.**)

51. Does the NM perform impact assessments of CSRDs, RFSs, TSRs, SAMs and TSOs? (**6.4.3.1.24.1.**)

52. Does the NM review, login, and research requests? (**6.4.3.1.24.2.**)

53. Does the NM provide technical advice and solutions for software, hardware and network connectivity; assist in the preparation of AF Forms 9, when required; create and maintain circuit layout records; update circuit and system labeling; complete in-house cross-connects and other minor device-to-demarcation point connections; and coordinate/perform initial test and acceptance on circuits? (**6.4.3.1.24.3.**)

54. Does the NM submit in-effect, exception, or delayed service reports as required, and develop and maintain a network circuit data base and network circuit history folders? (**6.4.3.1.24.4.**)

55. Does the NM perform ECO duties? (**6.4.3.1.25.**)

56. Does the NM verify equipment receipt, perform audits, and resolve and report known discrepancies? (**6.4.3.1.25.1.**)

57. Does the NM update the IPMS data base as required? (**6.4.3.1.25.2.**)

58. Does the NM issue equipment, perform initial and annual equipment inventory, and print and distribute inventory products? (**6.4.3.1.25.3.**)

59. Does the NM complete annual base-wide recertifications by account, monitor and assist unit ECs in ADPE responsibilities, monitor status of report of survey, prepare report of excess equipment, and complete paperwork for equipment turn-in? (**6.4.3.1.25.4.**)

60. Does the NM determine repair cost-effectiveness and submit cost estimate for equipment maintenance, process and monitor AF Forms 9 in conjunction with the plans and programs function, maintain a software library, and destroy excess commercial software? (**6.4.3.1.25.5.**)

61. Does the NM issue loaner equipment if available, set up and delete customer accounts, and provide EC training? (**6.4.3.1.25.6.**)

62. Does the NM perform contract management for base network support? (**6.4.3.1.26.**)

63. Does the NM consolidate and evaluate base-wide NCC managed network and system components as candidates for contract maintenance support? (**6.4.3.1.26.1.**)

64. Does the NM submit inputs to the unit plans and programs function for statement of work development? (**6.4.3.1.26.2.**)

65. Does the NM assist the plans and programs function in preparing the QASP and perform contract QAE functions as identified? (**6.4.3.1.26.3.**)

66. Does the NM perform base network budget planning? (**6.4.3.1.27.**)

67. Does the NM develop/submit budget input and request higher level funding for all NCC functions? (**6.4.3.1.27.1.**)

68. Does the NM monitor base network fund availability and process IMPAC requests for hardware and software purchases? (**6.4.3.1.27.2.**)

Fault Management:

1. Does the NM dispatch NCC or systems flight technicians to unmanned or user and subscriber locations when required to test, trouble-shoot, and restore service? (**6.4.3.2.1.**)

2. Does the NM coordinate with subscribers, local and distant support agencies, and contractors to isolate faults, restore service, and make repairs? (**6.4.3.2.2.**)

3. Does the NM ensure a trouble call process is established for each IS? (**6.4.3.2.3.**)

4. Does the NM monitor difficulty reports, heads-up messages, and system advisory notices? (**6.4.3.2.4.**)

5. Does the NM provide network and small computer maintenance support? (**6.4.3.2.5.**)

6. Does the NM maintain LRU stock level and assist users in ordering replacement LRUs? (**6.4.3.2.6.**)

7. Does the NM provide technical support to SAs when requested and maintain an electrostatic discharge maintenance area? (**6.4.3.2.7.**)

8. Does the NM perform fault isolation to the LRU and line item equipment level? Fault isolation methods include automated diagnostics and sound trouble-shooting techniques. (**6.4.3.2.8.**)

Performance Management:

1. Does the NM coordinate installation, acceptance testing, QA, fault isolation, and restoration of the communications infrastructure with the base's other communications unit functions? (**6.4.3.3.1.**)

2. Does the NM establish individual circuit and system parameters on non-DCS circuits and develop the parameters according to DISAC 300-175-9, supplemented by commercial-leased equipment and circuit performance standards? (**6.4.3.2.2.**)

3. Does the NM establish initial performance thresholds according to systems and circuit operation specifications and operational or mission requirements? (**6.4.3.3.3.**)

4. Does the NM integrate, configure, test, monitor, analyze, control, and restore systems to maintain top performance of intrabase and local support for DMC/RPC services? (**6.4.3.3.4.**)

5. Does the NM consolidate network performance data, security data, and analysis reports from all levels of the Air Force NM hierarchy? (**6.4.3.3.5.**)

6. Does the NM use the consolidated information to identify causes of service, performance, and security flaws? (**6.4.3.3.5.**)

7. On the basis of the aggregated analysis, does the NM recommend changes in network configurations, hardware or software, procedures, and staff training? (**6.4.3.3.5.**)

8. Does the NM remotely test subscriber equipment, end-to-end circuits, systems, and networks to verify the services provided and input and output signals meet standards? (**6.4.3.3.6.**)

9. Does the NM adjust remote network element equipment to optimize service? (**6.4.3.3.7.**)

10. Does the NM record configuration data, test data, failure symptoms, coordination efforts, fault isolation steps performed, and any other useful information? (**6.4.3.3.8.**)

11. Does the NM use this information to evaluate and control operations, service capabilities, and quality? (**6.4.3.3.8.**)

12. Does the NM report to management on quality of communication infrastructure services? (**6.4.3.3.9.**)

13. Does the NM perform system diagnostics and set global alarm thresholds and system parameters? (**6.4.3.3.10.**)

14. Does the NM monitor and optimize network performance? (**6.4.3.3.11.**)

15. Does the NM establish circuit and system parameters for non-DCS circuits? (**6.4.3.3.11.1.**)

16. Does the NM utilize NM performance tools to ensure optimum network operation, monitor system logs, analyze bandwidth use, and set global parameters to prevent the overall communications network from being adversely affected? (**6.4.3.3.11.2.**)

17. Does the NM ensure core systems have critical path redundancy? (**6.4.3.3.11.2.**)

18. Does the NM perform network/circuit QC testing and evaluation? (**6.4.3.3.12.**)

19. Does the NM generate and update QC schedules? (**6.4.3.3.12.1.**)

20. Does the NM plan, provide, coordinate, and verify alternate service during QC testing? (**6.4.3.3.12.2.**)

21. Does the NM have access to and monitor PMI schedules published by the maintenance control workcenter? (**6.4.3.3.12.3.**)

22. Does the NM coordinate in-service/out-of-service QC testing and specific area support performance of PMIs with affected workcenters and external agencies? (**6.4.3.3.12.4.**)

23. Does the NM coordinate and deactivate alternate service once testing/PMIs are completed and original circuit/equipment is verified operational? (**6.4.3.3.12.5.**)

24. Does the NM analyze QC performance trend analysis data (collected through NMS or out-of-service QC testing) to identify trends or patterns of circuit/system/network degradation, dispatch to and from user locations when required and generate and analyze outage reports? (**6.4.3.3.12.6.**)

25. In the absence of a PSCF, does the NM submit DD Forms 1368 when required and research, prepare, and submit QC waiver requests when necessary? (**6.4.3.3.12.7.**)

Security Management:

1. Does the NM enforce security policy by denying service and/or network connectivity? (**6.4.3.4.1.**)

2. Does the NM assist the wing IP office in developing a base-wide network security policy to effectively manage the base or wing network? (**6.4.3.4.1.**)

3. Does the NM assist the wing IP office in collecting information on accreditation packages for networks and systems on the base network infrastructure? (**6.4.3.4.2.**)

4. Does the NM ensure all systems and networks meet local security requirements and have appropriate DAA approval before connecting to the base network infrastructure? (**6.4.3.4.2.**)

5. Does the NM maintain historical documentation of all network and systems accreditation packages? (**6.4.3.4.2.**)

6. Does the NM perform information-gathering and vulnerability testing for base systems by conducting periodic vulnerability assessments of the base network? (**6.4.3.4.3.**)

7. Does the NM identify weak configurations and security holes by auditing and monitoring events occurring on the network? (**6.4.3.4.4.**)

8. Does the NM identify network intrusions by performing daily network analysis with USAF- approved intrusion detection tools? (**6.4.3.4.5.**)

9. Does the NM report all validated suspicious activity in accordance with AFSSI 5021? (**6.4.3.4.5.**)

10. Does the NM monitor audit and error logs for security violations and misuse? (**6.4.3.4.6.**)

11. Does the NM develop local procedures to report and respond to automated ISs and network stand-alone computer security and virus incidents according to AFSSI 5021? (**6.4.3.4.7.**)

12. Does the NM work with the wing IP office to identify internal actions such as local reporting channels, criteria for determining who is notified, etc.? (**6.4.3.4.7.**)

13. Does the NM ensure all network users are aware the NCC has the technical means available to monitor, capture, and record/store all transmissions traversing its network? (**6.4.3.4.8.**)

14. Does the NM identify and maintain a target baseline for Air Force-owned systems? (**6.4.3.4.9.**)

15. Does the NM install and set up audit tools and coordinate with global, regional, and wing IP offices? (**6.4.3.4.10.**)

16. Does the NM execute automated scripts to test vulnerabilities and execute vulnerability procedures where no scripts are available (e.g., NFS, NIS, cracking password, etc.)? (**6.4.3.4.11.**)

17. On systems accessed, does the NM test the configuration for vulnerabilities? (**6.4.3.4.11.**)

18. Does the NM collect data on intrusion activity and intrusion reporting by SAs and users? (**6.4.3.4.12.**)

19. Does the NM assist the SA in implementing countermeasures and firewall systems on targeted systems? (**6.4.3.4.13.**)

20. Does the NM perform AFCERT-directed changes? (**6.4.3.4.15.**)

21. Does the NM ensure ISs are accredited according to AFSSI 5024? (**6.4.3.4.16.**)

22. Does the NM conduct daily traffic analysis, identify and characterize incidents, generate incident reports, and forward reports according to AFSSI 5021? (**6.4.3.4.5.**)

23. Does the NM investigate each item to clarify and resolve suspicious activity? (**6.4.3.4.5.**)

24. Does the NM monitor base network architectures for effective automated security incident activity? (**6.4.3.4.5.**)

25. Does the NM maintain automated security incident historical transaction tapes and logs? (**6.4.3.4.17.**)

26. Does the NM respond to network security incidents and reports according to AFSSI 5021? (**6.4.3.4.5.**)

27. Does the NM perform security damage assessment? (**6.4.3.4.5.**)

28. Does the NM determine what data has been read, changed, or destroyed by unauthorized persons or machines? (**6.4.3.4.18.**)

29. Does the NM identify and secure computer systems on an affected network? (**6.4.3.4.18.**)

30. Does the NM identify computers where vulnerabilities are exploited? (**6.4.3.4.19.**)

31. Does the NM test for signs of hacker activity on other network systems? (**6.4.3.4.20.**)

32. Does the NM inform SAs and users on new systems security practices to prevent similar occurrences? (**6.4.3.4.20.**)

33. Does the NM brief incidents as required by applicable AFIs, AFCERT advisories, and AFSSIs, and provide technical support as requested? (**6.4.3.4.21.**)

Help Desk:

1. Does the HD monitor NM and system management system equipment? (**6.4.4.1.**)

2. Does the HD log on and off NM and system management systems? (**6.4.4.1.1.**)

3. Does the HD categorize, isolate, and resolve network problems? (**6.4.4.1.2.**)

4. Does the HD perform status checks and acknowledge alarms? (**6.4.4.1.3.**)

5. Does the HD generate NM and system management systems reports? (**6.4.4.1.3.**)

6. Does the HD maintain the operational data base? (**6.4.4.1.3.**)

7. Does the HD monitor the HD e-mail account and voice mail system? (**6.4.4.1.4.**)

8. Does the HD perform ad hoc queries? (**6.4.4.1.4.**)

9. Does the HD coordinate and respond to USAF, DISA, and Joint monitoring centers' directions? (**6.4.4.1.4.**)

10. Does the HD process trouble calls and coordinate problem resolutions? (**6.4.4.2.**)

11. Does the HD process and document customer trouble calls, monitor trouble ticket status, maintain trouble ticket data base, and create trouble ticket status reports? (**6.4.4.2.1.**)

12. Does the HD perform fault isolation by validating, isolating, and correcting faults and verify service restoral with customers? (**6.4.4.2.2.**)

13. Does the HD process scheduled and AOs? (**6.4.4.3.**)

14. Does the HD review AOs to determine base network service impacts and coordinate with local users? (**6.4.4.3.1.**)

15. Does the HD prepare and submit AO messages? (**6.4.4.3.1.**)

16. Does the HD review AO customer responses? (**6.4.4.3.1.**)

17. Does the HD maintain AO schedules? (**6.4.4.3.1.**)

18. Does the HD perform system checks after AOs are terminated? (**6.4.4.3.2.**)

19. Does the HD implement service restoral plans? (**6.4.4.4.**)

20. Does the HD authenticate restoral requests and implement required actions? (**6.4.4.4.1.**)

21. Does the HD verify service restoral? (**6.4.4.4.1.**)

22. Does the HD coordinate completion of restoral plans with appropriate agencies? (**6.4.4.4.1.**)

23. Does the HD prepare and submit formatted and unformatted reports? (**6.4.4.5.**)

24. Does the HD verify and submit required USAF and DISA reports on workcenter HAZCONs and major communications outages to appropriate agency? (**6.4.4.5.1.**)

Functional System Administrator:

1. Is the FSA qualified to perform the functions defined for all NM areas? (**6.4.5.1.**)

2. Has the FSA assumed responsibilities delegated by the NCC or CSO to optimize communications infrastructure performance and quality of service? (**6.4.5.1.**)

3. Has the FSA consolidated systems administration duties within an organization or a building, if possible, and merged them with the NCC based on a SLA? (**6.4.5.1.**)

4. Does the FSA ensure servers, workstations, peripherals, communications devices, and operating system/application software are properly configured for network operation, are on-line, and are available to customers? (**6.4.5.2.**)

5. Does the FSA perform NM duties in which the base network infrastructure components may be included? (**6.4.5.3.**)

6. Did the FSA establish contingency procedures, such as manual backup, reallocation of resources, and sharing assets, for systems critical to mission accomplishment? (**6.4.5.4.**)

7. Does the FSA periodically review the organization's needs for computer resources? (**6.4.5.5.**)

8. Does the FSA configure the operating system software to meet user needs (e.g., assigning user profiles, defining printer or modem access, and setting up user restrictions)? (**6.4.5.6.**)

9. Does the FSA define application ownership and determine who has permission to read, write, and execute? (**6.4.5.7.**)

10. Does the FSA assign and maintain logons, passwords, and user privileges on the system (e.g., which users share files)? (**6.4.5.8.**)

11. Does the FSA plan for short-term and long-term loss of system hardware and software? (**6.4.5.9.**)

12. Have the FSA and network security manager decided contingency plans in case of the FSA's absence. This may involve having another FSA administer the system remotely? (**6.4.5.9.**)

13. Does the FSA monitor the network and the system efficiency (e.g., finding and resolving system bottlenecks)? (**6.4.5.10.**)

14. Does the FSA perform routine system maintenance such as backing up or archiving files and adding software updates? (**6.4.5.11.**)

15. Does the FSA serve as the system trouble-shooter, a critical role in keeping the system operational, and contacting the NCC for hardware maintenance when necessary? (**6.4.5.12.**)

16. Does the FSA work with the NCC to set up network security policies and procedures? (**6.4.5.13.**)

17. Does the FSA monitor systems security and change passwords periodically? (**6.4.5.13.**)

18. Does the FSA train users when possible and contact the NCC for additional assistance? (**6.4.5.14.**)

19. Does the FSA provide user manuals that include sign-on and sign-off procedures, use of basic commands, software policies, user responsibilities, etc.? (**6.4.5.15.**)

20. Does the SA's area of responsibility include the user's terminal and the corresponding servers, but does not include the base network backbone infrastructure components? Some overlapping of responsibilities will occur. (**6.4.5.16.**)

21. Does the FSA maintain access control to the network and add, remove, and modify user profiles? (**6.4.5.16.1.**)

22. Does the FSA submit templates upon activation, register with the NIC, and request TAC-access user cards? (**6.4.5.16.2.**)

23. Does the FSA manage the MTA, the message store, and the DSA? (**6.4.5.16.3.**)

24. Does the FSA monitor daily e-mail activity and create and update NCC-controlled mail lists in the directory? (**6.4.5.16.4.**)

25. Does the FSA operate post regionalization (DMRD-924) DCP-40/50 front-end-processors, coordinate and provide media conversions, and provide distributed print management? (**6.4.5.16.5.**)

26. Does the FSA distribute standard and base-level software release documents to users? (**6.4.5.16.6.**)

27. Does the FSA maintain electronic bulletin boards and WWW home pages established by the NCC? (**6.4.5.16.7.**)

28. Does the FSA count and certify quantity of controlled products and distribute output products? (**6.4.5.16.8.**)

29. Does the FSA manage LAN and MAN directories; add, remove, and modify directory service; verify directory synchronization; and maintain the master data base? (**6.4.5.16.9.**)

30. Does the FSA download bulletin board information and distribute it? (**6.4.5.16.10.**)

Workgroup Manager:

1. Does the WM comply with systems administrator and NCC policies? (**6.4.6.2.**)

2. Does the WM perform the installation of equipment, connection of peripherals, and the installing/deleting of user software? (**6.4.6.3.**)

3. Does the WM configure user software, modify software configuration, and perform basic configuration management functions? (**6.4.6.4.**)

4. Does the WM set up and modify user introduction menus? (**6.4.6.5.**)

5. Does the WM perform bulk-loading/updating database files for resident application programs? (**6.4.6.6.**)

6. Does the WM perform database recovery for resident application programs? (**6.4.6.7.**)

7. Does the WM provide limited software application assistance for commonly used office automation applications purchased from standard Air Force infrastructure support contracts? (**6.4.6.8.**)

8. Does the WM perform e-mail address group maintenance; create, modify, and delete directories; move files from one media to another; and check files for corruption? (**6.4.6.9.**)

9. Does the WM perform initial system diagnostics and trouble-shooting of systems assigned to them? (**6.4.6.10.**)

10. Does the WM format, partition, backup and restore hard drives? (**6.4.6.11.**)

11. Does the WM create floppy boot disks? (**6.4.6.12.**)

12. Does the WM assign, modify, and delete passwords and user privileges? (**6.4.6.13.**)

13. Does the WM report security breaches, distribute security information, and perform risk analysis as necessary? (**6.4.6.14.**)

14. Does the WM send properly documented computer requirements to the base CSO for action? (**6.4.6.15.**)

15. Does the WM coordinate support issues with all agencies (e.g., customers, SA, NCC, etc.)? (**6.4.6.16.**)

16. Does the WM notify the unit ADPE EC of any hardware relocation? (**6.4.6.17.**)

17. Does the WM obtain an implementation checklist from the MAJCOM, CSO, NCC, and SA before installing equipment? (**6.4.6.18.**)

18. Does the WM assist with installing, testing, and accepting the system according to the terms of the purchase contract and instructions? (**6.4.6.18.**)

19. Does the WM isolate and resolve organizational computer problems within their own abilities, the FSA, and applicable service contract before seeking assistance from the NCC? (**6.4.6.19.**)

20. Does the WM inform the accountable ADPE EC of computer equipment problems? (**6.4.6.20.**)

21. Does the WM coordinate with the facility manager and the base civil engineer for facility support requirements? (**6.4.6.21.**)

22. Does the WM document technical support requirements on AF Form 332 and DD Form 1391? (**6.4.6.22.**)

23. Does the WM periodically review the organization's need for computer resources? (**6.4.6.23.**)

24. Does the WM identify training and manpower issues and/or needs? (**6.4.6.24.**)

25. Does the WM document integration and interoperability deficiencies and request help from the CSO? (**6.4.6.25.**) (***NOTE:*** If the problem does not lie within the capabilities of the CSO, users may have to fund for integration/interoperability problem resolution from a contracted source.)

26. Does the WM validate computer equipment requirements the unit ADPE EC submits? (**6.4.6.26.**)

27. Does the WM assist the unit ADPE EC with computer hardware and software inventories? (**6.4.6.27.**)

28. Does the WM work with the FSA to ensure NM procedures comply with contracting documents? (**6.4.6.28.**)

29. Does the WM send all software with documentation that costs more than $5,000 or requires more than 40 man-hours to develop, to the base CSO for inclusion in the Defense Integration Support Tool and possible use or reuse by other organizations? (**6.4.6.30.**)

30. Does the WM ensure the organization develops and maintains software according to MAJCOM guidance? (**6.4.6.31.**)

31. Does the WM report computer resources to the organization ADPE EC at least 120 days prior to the equipment becoming excess? (**6.4.6.32.**)

32. Does the WM promote user awareness concerning unauthorized or illegal use of computer hardware and software? (**6.4.6.33.**)

33. Does the WM identify organization deficiencies and operational needs that computer use can solve? (**6.4.6.34.**)

34. Does the WM plan support for deployments (see AFIs 10-403 and 33-104)? (**6.4.6.35.**)

35. Does the WM notify the CSO of maintenance requirements for computers? (**6.4.6.36.**)

36. Does the WM establish maintenance reporting procedures according to instructions provided by the CSO? (**6.4.6.37.**)

37. Does the WM ensure organizations do not use shareware or public domain software until the CSO certifies it to be free of viruses, hidden defects, and obvious copyright infringements? (**6.4.6.38.**)

38. Does the WM ensure organizational shareware users pay any necessary fees? (**6.4.6.39.**)

39. Does the WM ensure correct management of records created by or stored on computers by coordinating with the unit records manager? These records include information for official use only or information subject to the Privacy Act of 1974. (**6.4.6.40.**)

Training:

1. Does the NCC work with AETC to create and modify training modules and learning guides as you install or modify systems and services, and when you receive initial contractor training? (**7.2.**)

2. Does the NCC ensure the training modules and learning guides conform to instructional systems development standards? (**7.2.**)

3. Does the NCC qualify entry-level personnel to perform tasks as journeymen and supervisors and support follow-on qualification training and certification? (**7.2.**)

4. The NCC should not modify nor eliminate training modules and learning guides just because all assigned personnel are currently qualified. (**7.2.1.**)

5. Does the NCC use AFI 36-2201 to guide training program development, implementation, and maintenance? (**7.2.2.**)

6. Does the NCC reduce the need for local training modules or learning guides by using Air Force on-the-job training products (see AFIND 8)? (**7.3.**)

7. If existing Air Force job qualification standards or qualification training packages are not adequate, does the NCC supplement them with local guides? (**7.3.**)

8. Do the NCC personnel receive general and technical information protection training? (**7.4.**)

9. Does the NCC obtain training either from the AETC formal courses, through distance learning training, or on-the-job training products? (**7.4.**)

10. Does the NCC use all possible avenues of training delivery to achieve and maintain quality of service? (**7.5.**)

11. AETC resident and field training detachment courses may not provide all the training needed at every location in the Air Force. Does the NCC fill the gaps with commercial training and unit-sponsored seminars and courses? (**7.5.**)

12. Does the NCC ensure that people who attend commercial training courses develop training modules and learning guides? (**7.5.**)

13. Does the NCC keep all commercial course materials and use them to deliver follow-on training? (**7.5.**)

14. Does the NCC ensure NM areas subordinate to the NCC (i.e., FSA and WM) receive adequate training prior to being assigned duties in any NM area? (**7.6.**)

15. Does the NCC provide education and training to base computer users? (**7.7.**)

16. Does the NCC ensure each operator, WM, and FSA receives a level of instruction commensurate with his/her duties and responsibilities? (**7.7.1.**)

17. Does the NCC draft and forward customer education letters or handbooks, conduct customer training surveys, and advertise training availability? (**7.7.2.**)

18. Does the NCC prepare training outlines and course material, train instructors, prepare class schedules, schedule customers for training, configure computers for specific courses, and conduct customer training classes? (**7.7.3.**)

19. Does the NCC conduct evaluations to see if training meets the customers' needs and develop and maintain a base reference library for hardware and software applications? (**7.7.4.**)

20. Does the NCC educate FSAs, WMs, and other base customers in network services, fault isolation, security, and trouble reporting? (**7.7.5.**)

21. Do NCC personnel visit user organizations to stay familiar with user requirements? (**7.7.6.**)

Attachment 6

IC 99-1 TO AFI 33-115V1, NETWORK MANAGEMENT

2 JULY 1999

SUMMARY OF REVISIONS

This change incorporates IC 99-1. It ensures all systems are properly configured with required security patches, correct versions of all software, and a test/validation is performed off-line before restoring to operations. This is a significant step forward in our network operational posture and should lead to improved computer network security. A (|) indicates revision from the previous edition.

6.4.2.11. Implements software patches and security fixes as required by the NCC, NOSC, AFCERT, AFNOC, or program manager. Tests and validates the proper operation and configuration with appropriate patches and fixes, as required above, prior to restoring any device to the network.

6.4.5.17. Implements software patches and security fixes as required by the NCC, NOSC, AFCERT, AFNOC, or program manager. Tests and validates the proper operation and configuration with appropriate patches and fixes, as required above, prior to restoring any device to the network.